Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Facultad de Ingeniería de Sistemas e Informática

Escuela Académico Profesional de Ingeniería de Sistemas

Sistema de protección de archivos de constitución de empresas haciendo uso de la tecnología de firma digital

TESINA

Para optar el Título Profesional de Ingeniero de Sistemas

AUTORES

Duilio Eduardo DE LA MOTTA PAEZ

Luis Harold VELA BERROCAL

ASESOR

Luis Ricardo ROIG DEL ALCÁZAR

Lima, Perú

2008

Referencia bibliográfica

De la Motta, D. & Vela, L. (2008). *Sistema de protección de archivos de constitución de empresas haciendo uso de la tecnología de firma digital*. Tesina para optar el título profesional de Ingeniero de Sistemas. Escuela Académico Profesional de Ingeniería de Sistemas, Facultad de Ingeniería de Sistemas e Informática, Universidad Nacional Mayor de San Marcos, Lima, Perú.

“SISTEMA DE PROTECCIÓN DE ARCHIVOS DE CONSTITUCION DE EMPRESAS HACIENDO USO DE LA TECNOLOGÍA DE FIRMA DIGITAL”

RESUMEN

Esta tesina pretende mostrar una forma diferente de incorporación de la tecnología de certificados digitales orientada a documentos sensibles combinando formatos digitales y analógicos para lo cual se ha desarrollado un sistema de encriptación y verificación que incorpora tecnología de contenedores digitales aplicando el esquema de llaves pública y privada.

La aplicación permite la manipulación de la información en repositorios seguros, el envío por medios digitales garantizando la inviolabilidad e integridad de la información y la verificación del formato en papel como respaldo de origen de su par en formato digital.

PALABRAS CLAVES

Firma digital, certificados digitales, claves públicas, claves privadas, smart card.

"CONSTITUTION FILE PROTECTION SYSTEM USES DIGITAL SIGNATURE TECHNOLOGY"

ABSTRACT

This thesis aims to show a different way of incorporating digital certificates technology aimed at sensitive documents combining digital and analog formats that has developed an encryption system that incorporates technology and verification of digital containers applying the scheme of public and private keys.

The application allows to manipulate information in safe repositories, also sending digital media by ensuring information inviolability and integrity and verificate the paper form as an endorsement of its original copy in digital format.

KEYWORDS

Digital signature, digital certificates, public keys, private keys, smart card.

A mis padres, con mucho cariño y admiración.

Eduardo

Gracias a mis padres
por toda su confianza y comprensión

Luis

UN AGRADECIMIENTO PROFUNDO AL NUESTRO ASESOR LIC. LUIS ROIG DEL ALCAZAR POR SU EXPERIENCIA, COLABORACIÓN Y DISPOSICIÓN PARA REALIZAR ESTA INVESTIGACIÓN

INDICE

PARTE I – EVALUACION DE TESIS 10
1.1 INTRODUCCION 11
1.2 ANTECEDENTES 12
1.3 DEFINICIÓN DEL PROBLEMA 13
1.4 OBJETIVOS 13
1.5 ALCANCE DEL PROYECTO 14
1.6 LIMITES DEL PROYECTO 14
1.7 JUSTIFICACIÓN 14
1.8 PROPUESTA 15
1.9 ORGANIZACIÓN DE LA TESINA 16
PARTE II – MARCO TEORICO 18
2.1 CRIPTOLOGIA 19
2.2 CRIPTOGRAFIA 19
2.2.1 CRIPTOGRAFIA SIMETRICA 21
2.2.2 CRIPTOGRAFIA ASIMETRICA 21
2.3 ESTEGANOGRAFIA 23
2.4 HASHING 24
2.4.1 ALGORITMO MD5 26
2.4.2 ALGORITMO SHA 26
2.5 PLATAFORMA DE DESARROLLO 27
2.5.1 .NET FRAMEWORK 28
2.5.2 VISUAL BASIC 30
2.6 METODOLOGIAS DE DESARROLLO 30
2.6.1 SCRUM 30
2.6.2 XP 31
2.6.3 UML 33
2.7 ORGANIZACIONES INVOLUCRADAS 34
2.7.1 VENTANILLA UNICA DEL ESTADO 34
2.7.2 NOTARIAS 36
2.7.3 PROINVERSION 37
2.7.4 SUNARP 37
2.7.5 SUNAT 38
PARTE III – ESTADO DEL ARTE 39
3.1 FIRMA DIGITAL 40
3.1.1 TIPOS DE FIRMA DIGITAL 40
3.1.2 ¿CÓMO FUNCIONA LA FIRMA DIGITAL? 42
3.1.4 PKI - INFRAESTRUCTURA DE CLAVE PÚBLICA 44
3.1.5 CERTIFICADOS DIGITALES 47
3.1.6 TARJETAS INTELIGENTES (SMART CARDS) 49

3.1.7 LLAVES ETOKEN 50
3.2 MARCO LEGAL DE LA FIRMA DIGITAL EN EL PERU 51
PARTE IV - DESARROLLO DE LA SOLUCION 53
4.1 AMBITO DE LA SOLUCION 54
4.1.2 PARTICIPACION DE LOS ORGANISMOS 54
4.2 ARQUITECTURA DEL SISTEMA 60
4.3 DESCRIPCION DE LA SOLUCION 63
4.3.1 ENCRIPTADOR 63
4.3.2 VERIFICADOR 64
4.4 DIAGRAMAS UML 64
4.5 USO DE LAS METODOLOGIAS 77
4.5.1 APORTE DE SCRUM 77
4.5.2 APORTE DE XP 79
4.6 DESCRIPCION DE SOFTWARE PROPUESTO 80
4.6.1 APLICACIÓN ENCRIPTADOR 80
4.6.2 APLICACIÓN VERIFICADOR 96
PARTE V - CONCLUSIONES 106
PARTE VI - REFERENCIAS BIBLIOGRAFICAS 109
INDICE DE FIGURAS 113
PARTE VIII - ANEXOS 114

PARTE I – EVALUACION DE TESIS

1.1 INTRODUCCION

En estos momentos nos encontramos inmersos en un proceso de transformación social, económica y empresarial, motivado por la disponibilidad de nuevas tecnologías. Estas son la base para el lanzamiento de nuevos tipos de negocio, que pueden existir para potenciar los negocios tradicionales.

Hemos tenido una transformación económica en los últimos años la cual ha llegado a la evolución de la economía digital, involucrando una drástica transformación de los modelos de negocios tradicionales ya que no se requiere la presencia física de las partes, los tiempos se acortan, además las estrategias se orientan a la entrega de herramientas interactivas a los clientes, se produce un cambio cultural respecto a soportes materiales como papel, formularios, firmas, concurrencias a notarias y diversos trámites de alto costo y demora.

Otro hecho, que sin duda refuerza toda esta nueva tendencia digital, fue la aprobación de la Ley sobre Firma Digital (LEY Nº 27269) ya que abren un camino más seguro a la celebración de actos y contratos, envío de documentación y comercio por vía electrónica, constituyendo un significativo respaldo e impulso a estas transacciones.

De acuerdo a esta ley y con la sola exclusión de los documentos que requieran de solemnidades diferentes o adicionales, o la comparecencia personal para ser extendidos, o estén relacionados con el derecho de familia-, los actos y contratos otorgados o celebrados por personas naturales o jurídicas, suscritos por medio de firma electrónica, serán tan válidos y producirán los mismos efectos que los celebrados por escrito y en soporte de papel. De hecho, estos actos y contratos se reputarán como escritos, en los casos en que la ley exija que los mismos consten de ese modo, y en todos aquellos en que prevea consecuencias jurídicas cuando figuran por escrito.

La firma electrónica se puede definir como un código que las personas o entes públicos y privados obtendrán cuando se inscriban ante una empresa certificadora, la que puede ser acreditada o no acreditada.

Con esta solución se busca mejorar el trámite de constitución de empresas, dotándolo de mecanismos de seguridad que eviten la clonación y/o falsificaron de constitución de empresas con fines delictivos

Esto facilitará el comercio, la realización de trámites, las compras electrónicas y las transacciones entre privados, empresas o instituciones, asignando un valor legal indiscutible a las millones de transacciones electrónicas que hoy se realizan en el país a través de la comprobación de la autenticidad de dichas escrituras de constitución de empresas que son de carácter público.

Al eliminar los riesgos de seguridad y de identidad de los usuarios, la firma digital ayudará a masificar el uso de Internet y a disminuir la utilización del papel, acarreando una indudable mejora tanto en la calidad como en la velocidad del tráfico jurídico y comercial. También permitirá grandes ahorros a las organizaciones, ya que los costos de los procesos electrónicos son mucho menores que los de los físicos y presenciales.

En la medida que las organizaciones y empresas comprendan y apliquen las ventajas que otorga esta nueva herramienta, podrán prestar un mejor y más veloz servicio. En este sentido, nos enfrentamos a un gran desafío, porque una cosa es haber logrado la aprobación de la ley, y otra muy diferente es cambiar la cultura y las prácticas de las instituciones.

Ante estas nuevas herramientas disponibles, nace la inquietud de evaluar el impacto de estas nuevas tecnologías en los negocios, con especial énfasis en lo que se refiere a la Constitución de Empresas en Línea.

1.2 ANTECEDENTES

Entre los antecedentes que se pueden contar dentro de la aplicación de la tecnología de firma digital en nuestro país se encuentra el utilizado por la CONASEV (Comisión Nacional Supervisora de Empresas y Valores del Estado Peruano) a través del sistema MVNET (http://mvnet2.conasev.gob.pe/mvnet/inicio.htm) el cual permite el intercambio de información segura y eficiente, entre las entidades

obligadas y CONASEV. El punto de partida fue el uso de la tecnología PKI desde el año 2003, como una iniciativa de la organización amparada bajo la Resolución CONASEV Nº 008-2003-EF/94.10.

Otro antecedente se remonta al año 2004, por Resolución de la SUNAT, N°201-2004/SUNAT (http://www.sunat.gob.pe/legislacion/superin/2004/201.htm) se fija otro precedente para el uso de la Firma Digital en organismos del Estado pues se implementa un sistema de notificación de embargos que interactúa con empresas del sistema financiero de forma electrónica. Este sistema se le conoce como SEMT (Sistema de Embargo por Medios Telemáticos).

1.3 DEFINICIÓN DEL PROBLEMA

Carencia de herramientas para validar una escritura pública de Constitución de Empresas que eviten una falsificación o clonación de la misma entre las diferentes instituciones que interactúan en el proceso de Constitución de Empresas en nuestro país.

Esta problemática ocurre con todos aquellos documentos que tienen carácter de Escritura Pública y son visados por los Notarios.

1.4 OBJETIVOS

- Desarrollar una solución informática para resolver el problema de validación y generación de Escrituras Públicas de Constitución de Empresas a través de la técnica firma digital.
- Reducir tiempo, recursos humanos y costos en el proceso de Constitución de Empresas.
- Lograr un eficaz intercambio de información entre las entidades que forman parte de ciclo de constitución de empresas (RENIEC, SUNAT, SUNARP, CNL y otros), alineándose de esta manera a la implementación de Ventanilla Única del Estado que forma parte de la iniciativa de Gobierno Electrónico del país.

1.5 ALCANCE DEL PROYECTO

El alcance del presente Proyecto es lograr el intercambio de información electrónica en tiempo real entre y hacia las instituciones públicas involucradas en dicho proceso (Constitución de Empresas), mediante la integración de la información, la implementación de mecanismos de seguridad y la utilización de medio de pagos electrónicos.

1.6 LIMITES DEL PROYECTO

Los límites que podrían darse dentro de estos proyectos son:

- Un largo y tedioso proceso de negociación entre las diferentes instituciones públicas involucradas a nivel de competencias, funciones y definición de estándares entre ellas.
- Generar el cambio de voluntades en la cultura organizacional de las instituciones públicas.
- Una reforma general de sus procesos a través de un respectivo Análisis de Procesos que se debe dar entre las oficinas de proceso encargadas con la gente encargada de Sistemas.
- Lograr planes efectivos y desarrollados de descentralización.
- Lograr un desarrollo y fortalecimiento de las capacidades de las instituciones públicas.

1.7 JUSTIFICACIÓN

El interés en el desarrollo de esta tesina fue motivado bajo dos criterios:

Impacto en la organización

El uso de la tecnología de firma digital es incipiente en nuestro país y se consideró interesante hacer un aporte que establezca un referente en el uso de esta herramienta tecnológica que es replicable a otros documentos que se puedan utilizar en el Estado o sector privado.

Esto debe ir acompañado de una adecuada campaña de información para el cambio de una "cultura de papel" a una cultura digital.

Impacto tecnológico

El hecho de implantar esta tecnología involucra conceptos relacionados a la seguridad, como la encriptación, protección de datos, transmisión de los mismos e integración con sistemas de otras instituciones, lo cual genera una perspectiva integral de la generación de documentos electrónicos validos.

1.8 PROPUESTA

La propuesta planteada en este trabajo de investigación está conformada por una solución informática centrada en el aspecto de la firma digital y las tecnologías complementarias, buscando un manejo transparente y sencillo a los usuarios y/o instituciones que participan en el proceso.

La solución informática muestra las siguientes funcionalidades:

- Generación de documentos electrónicos con firma digital que poseen características de autenticidad, integridad y no repudio.

- Importación de documentos electrónicos de fuentes externas para ser firmados digitalmente por las notarias.

- Exportación y transmisión de documentos electrónicos a otros sistemas para propósitos de validación.

- Visualización e impresión de los documentos electrónicos del sistema.

- Utilización de la tecnología de certificados digitales para lograr la confidencialidad en la transmisión de la información.

Nuestra propuesta está centrada en el caso del proceso de Constitución de Empresas, el cual se puede ampliar a otros procesos existentes en el ámbito notarial.

A nivel tecnológico la solución informática es una aplicación de tipo StandAlone, basada en la plataforma NET Framework 2.0 y desarrollada en Visual Studio .NET que integra las siguientes tecnologías:

- Cifrado y verificación de documentos utilizando 2D SIS contenidas en un SDK de fabricación eslovaca.
- Llaves Etoken.
- Smart Card.
- Certificados digitales.
- Hashing.

1.9 ORGANIZACIÓN DE LA TESINA

La presente investigación está organizada por secciones. La primera sección comprende el marco teórico, donde se desarrollan temas relacionados con la criptología como la criptografía, hashing y algoritmos. De forma complementaria, se ha descrito la plataforma tecnológica sobre la cual se ejecuta la aplicación y la metodología de desarrollo. Hemos sumado a esto la descripción de las organizaciones que participan en la solución.

Centrándonos en el punto de Firma Digital, se optado por definir conceptos claros y sencillos que apunten a tener una guía para implementación de forma general, así como definiciones de certificados digitales y el hardware relacionado. Adicionalmente se complementa con el marco legal existente en nuestro país.

A continuación se desarrolla la solución, presentando antes de la misma el contexto donde funciona la aplicación motivo de la tesina, pues este proyecto es parte de una solución integral. Seguidamente, se describe la solución desde el punto de vista teórico y finalizando con la explicación del software desarrollado.

Para terminar, realizamos las conclusiones, donde mostramos el impacto de la solución y sus posibilidades. Complementamos esta tesina con anexos relacionados al ámbito legal y que son el marco de las futuras aplicaciones de firma digital en nuestro país.

PARTE II – MARCO TEORICO

2.1 CRIPTOLOGIA

La criptología cuyas áreas de interés son la criptografía el criptoanálisis, y la esteganografía es la ciencia que estudia los sistemas criptográficos.[3]

La criptografía es el método que consiste en transformar un texto entendible en un criptograma (texto cifrado) cuya información solo lo entienden aquellas personas que poseen la clave para descifrarlo.[2]

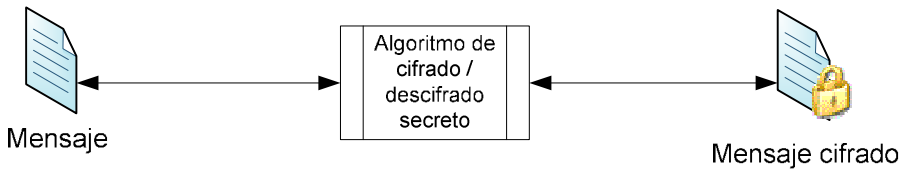
El criptoanálisis es el conjunto de técnicas o métodos para descifrar los criptogramas sin la tenencia de una clave.

2.2 CRIPTOGRAFIA

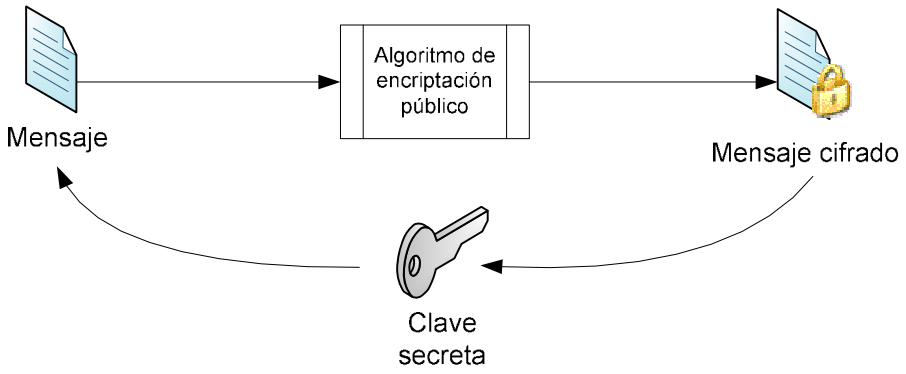
Este mecanismo de protección de información usado desde la Edad Antigua hasta la actualidad proviene de dos vocablos griegos: “kripto” (ocultar) y “graphos” (escribir) los cuales se pueden interpretar como “escritura oculta” resumen el concepto de la criptografía que consiste en la utilización de técnicas para cifrar y descifrar información que es entendida por las personas autorizadas.

Para cifrar un texto mediante una técnica se debe utilizar una función inversa que conocen las personas responsables de la información. Frecuentemente esta función inversa implementada a través de un algoritmo ya sea privado o público que complementada con la clave permite el cifrado o descifrado (encriptación o desencriptación) de la información.

Es importante mencionar que los objetivos principales de la utilización de esta técnica es mantener en secreto la información transmitida y que dicha información la recibe la persona indicada.



Aquí lo importante es el algoritmo, ausencia de clave.



Se suma la presencia de la clave.

Figura 2.1 Ejemplos de encriptación

En la actualidad los sistemas emplean algoritmos públicos y claves secretas por las siguientes ventajas:

- Transmitir la clave es más seguro y sencillo que el funcionamiento del algoritmo público.

- Los algoritmos de uso público pueden incorporarse en el hardware y aplicaciones abaratando el costo de la implementación.

- Los algoritmos públicos son probados por la comunidad científica buscando vulnerabilidades. Un algoritmo secreto puede ser susceptible a fallos y un criptoanalista puede aprovecharse para la obtención de la información.

Los lenguajes o entornos de programación en la actualidad como PHP, .NET u otros incorporan clases o librerías para cifrado y descifrado de información.

2.2.1 CRIPTOGRAFIA SIMETRICA

Este método se caracteriza por usar en el cifrado y descifrado de información la misma clave. ¿Dónde está el riesgo aquí? Pues en el mecanismo de intercambio de claves. De hecho lo que buscaría un atacante no es encontrar la clave sino interceptar el canal de comunicación de la clave.

A esto se suma el hecho que si nos comunicamos con muchas personas usando esta técnica cada una necesitaría una clave y si quisiéramos una red privada de intercambio de información para n personas se necesitarían n(n-1)/2 claves en el sistema. Dicho de manera práctica si tenemos una red de 10 personas en el sistema de comunicación existirían 45 claves para lograr una comunicación privada de 1 a 1. Algunos ejemplos de algoritmos simétricos son DES, 3DES (DES Múltiple), AES, Blowfish, RC5, CAST e IDEA. Los algoritmos simétricos suelen usar complejidades que oscilan entre los 64 y 512 bits.

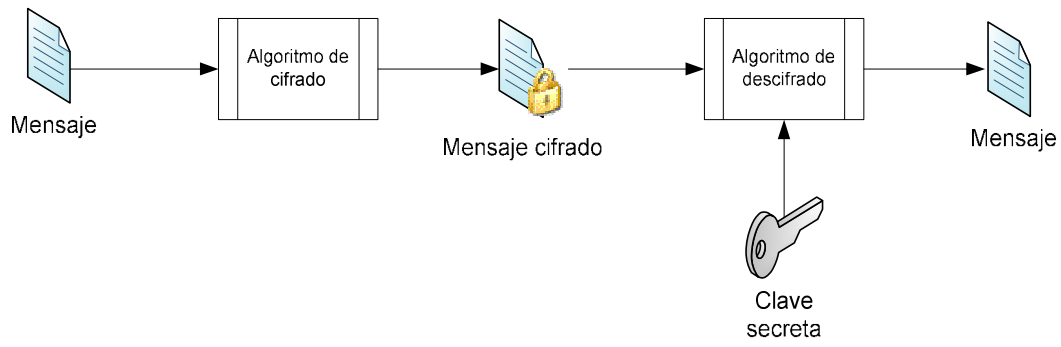


Figura 2.2.1 Criptografía simétrica

2.2.2 CRIPTOGRAFIA ASIMETRICA

También conocida como criptografía de clave pública, se basa en las propiedades matemáticas de los números primos. En este sistema existen dos claves, una secreta o privada y la clave pública. La primera como su nombre lo dice es secreta, no se transmite y nadie debe tener acceso a la misma. La segunda es pública y se puede

entregar a cualquiera, a esto hay que añadir que es imposible obtener la clave pública de la privada.

Con este sistema de cifrado logramos la confidencialidad. Cualquier intruso que intercepte la transmisión no podrá descifrar el contenido de la misma al no poseer la clave privada del receptor.

Este mecanismo de cifrado se inventó con el objeto de evitar por completo el problema del intercambio de claves ocasionados por la criptografía simétrica y fueron concebidos en los 70s por los matemáticos Whitfield Diffie, Martín Hellman y el informático Ralph Merkle.

En la criptografía asimétrica es frecuente el uso de una cantidad de bits mucho mayor con respecto a la criptografía simétrica. Por lo que la posibilidad de encontrar la clave se reduce enormemente. Por ejemplo en el algoritmo simétrico de 128 bits, esto significaría que existen $2^{128} – 1$ claves posibles. En cambio para los algoritmos asimétricos se recomiendan claves de 1024 bits en adelante, incrementando la cantidad del trabajo para los intrusos que quieran averiguar la clave.

El incremento del número de bits y la complejidad propia de los algoritmos asimétricos durante el procesamiento de las claves hace sea más lento que sus pares simétricos, a mayor longitud de clave, más tiempo de proceso.

Otro inconveniente con respecto a los algoritmos simétricos es que el mensaje cifrado ocupa más espacio que el mensaje original. Es por eso que al usar este sistema la cantidad de datos transmitidos debe ser pequeña.

Entre los principales algoritmos están el Diffie – Hellman, RSA, Curvas Elipticas, DSA, ElGamal.

Entre los protocolos de comunicación que usan claves asimétricas están: GPG, PGP, SSL, SSH, entre otros.

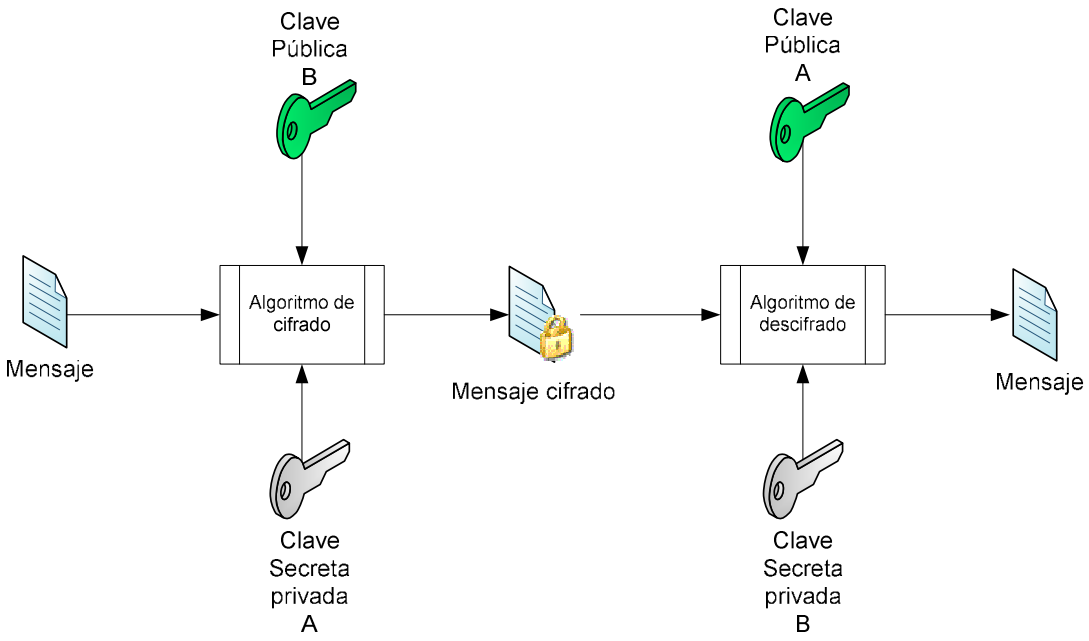


Figura 2.2.2 Criptografía simétrica

2.3 ESTEGANOGRAFIA

La esteganografía es una parte de la criptología que utiliza métodos para ocultar mensajes dentro de otros mensajes, imágenes, objetos u otros. Es decir el "portador" del mensaje no necesariamente es del mismo tipo o aspecto que la información transmitida.

Veamos un ejemplo práctico, suponga usted qué quiere ocultar el nombre de la ciudad donde se encuentra un tesoro y para eso utiliza la oración: "Allá recordarás eso que uno intenta pintar aquí". ¿Tiene lógica? Aparentemente si, y probablemente la expresión pasaría entre sus amigos sin darse cuenta del mensaje. Pero si uno escoge la primera letra de cada palabra de la oración se dará con la sorpresa que dice "Arequipa".

Hagamos más interesante el desafío, suponga que sabe las coordenadas exactas y las quiere adicionar en el mensaje. Entonces con una impresora especial añade las coordenadas en una microimpresión en el punto de la "i". Eso es esteganografía.

En los últimos años la esteganografía ha obtenido un gran interés pues se sospecha que dicha tecnología es usada por terroristas para comunicar planes de ataques que sucederían en el futuro. Imagine como sería camuflar una frase o pequeños datos en una imagen JPG de una pintura que tiene millones de pixels y colores.

La ciencia que se dedica al estudio de los mensajes ocultos mediante la esteganografía se le conoce como estegoanálisis.

2.4 HASHING

El hashing es una técnica en la cual se aplica una función hash con el propósito de generar una clave que represente al documento de manera univoca esto quiere decir que la clave solamente puede ser generada por un documento y nada más. Puede suceder que se generen claves iguales para objetos diferentes (colisión), esto ocurre si el rango de claves que se podrían generar es menor que el de posibles objetos a resumir. [4]

Un ejemplo de colisión es el siguiente y se da en las redes Peer to Peer (P2P), imagine que alguien comparte un archivo que es muy grande (10 Gigabytes) y el protocolo de compartición de datos establece que los paquetes de transmisión de datos es de 32 Kilobytes. Si hacemos la división correspondiente se tendría que transmitir 10 485 760 paquetes. Si la función hash que usted emplea solo puede generar 8 millones de claves, en consecuencia, diferentes paquetes de datos estarán asociados a un mismo hash porque el número de claves que provee la función es insuficiente. El resultado es que el archivo destino que está llegando a su computador no será igual al archivo origen. Una buena función de hash genera pocas colisiones.

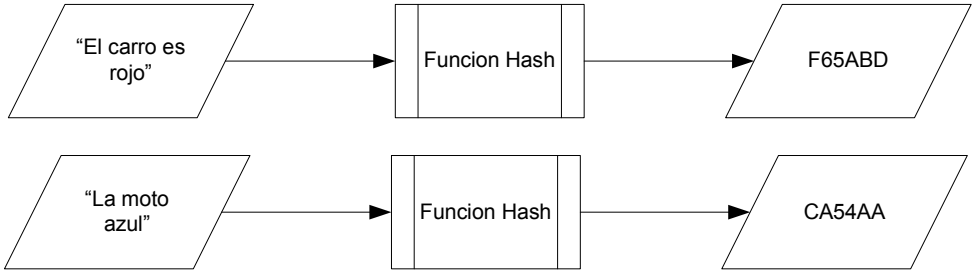


Figura 2.4 Hashing

Una función hash resume o identifica datos a través de la probabilidad matemática. Entre sus aplicaciones se encuentran la reanudación de la transferencia de archivos en redes P2P como BitTorrent o Gnutella. La verificación CRC de los paquetes de datos transmitidos y en el archivo final. Esto último es para verificar si el archivo grabado es realmente el archivo publicado por el fabricante y no se encuentre modificado.

En programación se suelen utilizar las tablas hash, las cuales son una colección de claves, las que están asociadas cada una a un registro específico. Esto acelera la capacidad de búsqueda de registros de manera notable.

En criptografía, el hashing se utiliza para firmar los mensajes y archivos. Firmar significa calcular un valor hash en base a los datos de entrada. Una vez firmado el mensaje, si alguien altera el contenido será puesto en evidencia porque el valor hash no coincidirá con el que se calcule al momento de descifrarlo.

Entre las propiedades del hashing tenemos:

- Es imposible reconstruir el mensaje original a partir de la clave hash.
- Todas las claves generadas con una función de hash tienen el mismo tamaño, sea cual sea el mensaje utilizado como entrada.
- Es fácil y rápido determinar la clave de un mensaje usando computadoras.

Existen muchos algoritmos para calcular una función hash. Entre ellos están el MD4, MD5, SHA, Tiger, etc.

2.4.1 ALGORITMO MD5

Este algoritmo fue desarrollado en 1991 por Ron Rivest, criptógrafo del MIT, para reemplazar otra función de hash llamada MD4. El nombre de este algoritmo proviene de "Message-Digest Algorithm 5"[5] ha sido utilizado en un extenso rango de aplicaciones relacionadas a seguridad y es frecuentemente usado para verificar la integridad de los archivos.

La codificación del MD5 de 128 bits es representada típicamente como un número de 32 dígitos hexadecimales. Un ejemplo de esto es:

d8ef2e04292738e0d42d09c8bc0238e4 = MD5 ("Prueba del algoritmo MD5")

En el año 1996, Dobbertin (quien diseñara el algoritmo MD4) descubrió una colisión de la función de compresión del MD5, sin embargo no fue considerado un ataque completo de la función MD5. Sin embargo, los criptógrafos comenzaron a recomendar el uso de otros algoritmos como el SHA-1. El año 2004, los científicos chinos Xiaoyun Wang y Hongbo Yu encontraron una falla de colisiones completa en el diseño del MD5 e hicieron una prueba de concepto que completaron en una hora usando un cluster de IBM p690[36]. El año 2005, más fallas fueron descubiertas por Arjen Lenstra, Xiaoyun Wang, Benne de Weger probaron que dos certificados x.509 podían tener la misma clave hash (colisión)[37].

2.4.2 ALGORITMO SHA

Las funciones hash SHA[6] son cinco funciones criptográficas diseñadas por la Agencia Nacional de Seguridad de los Estados Unidos (NSA) y publicadas por el

Instituto Nacional de Estándares y Tecnologías (NIST). El termino SHA proviene de "Secure Hash Algorithm", que se puede traducir como Algoritmo de Hash Seguro. Esta familia está compuesta por los algoritmos SHA-1, SHA-224, SHA-256. SHA-385 y SHA-512.

Un ejemplo de una clave hash SHA-1 es:

57f1aebd906808c1738b0dd03680cd3e6401dbe7 = "Prueba del algoritmo SHA-1"

Se le conoce como SHA-0 al primer algoritmo de la familia SHA. Como consecuencia de la aparición de colisiones se mejora este algoritmo, convirtiéndose así en el SHA-1. Al resto de algoritmos (SHA-224, SHA-256. SHA-385 y SHA-512) se les conoce como SHA-2.

El algoritmo SHA-1 (y el SHA-0) producen un hash de 160 bits de un mensaje que puede tener un tamaño de hasta 264-1 bits y el principio matemático es semejante al diseño del MD4 y MD5. Los algoritmos del tipo SHA-2 producen un hash igual al número de bits que acompaña al termino "SHA". Esto quiere decir que el algoritmo SHA-256 genera un hash de 256 bits.

SHA-1 es utilizado en una extensa variedad de protocolos y aplicaciones relacionadas a la seguridad entre las que se incluyen el TLS, SSL, PGP, SSH, firma digital y otros. Es considerado para ser el sucesor del MD5.

La seguridad del SHA-1 se vió comprometida en la investigación hecha por Bruce Schneir[7]. Hasta la fecha no se tiene noticias de vulnerabilidades o fallas en las variantes del SHA-2.

2.5 PLATAFORMA DE DESARROLLO

2.5.1 .NET FRAMEWORK

También conocida como .NET. Esta plataforma desarrollada en los últimos años por la empresa Microsoft como evolución del API Win32 es la respuesta a la plataforma Java de Sun Microsystems. Tiene por objetivo el acceso sencillo a cualquier tipo de datos desde cualquier dispositivo y una mayor y rápida integración de los sistemas en los negocios.

A nivel tecnológico lo que está consiguiendo .NET es una integración horizontal de sus productos de software, buscando un desarrollo unificado y un fácil intercambio de datos.

Entre los componentes del .NET Framework[8] están:

- El motor de aplicaciones CLR (Common Language Runtime), es la parte de .NET encarga de procesar el código intermedio llamado "MSIL", compilarlo en tiempo real (Compilador "JIT") y generar el código máquina que entiende el computador. Esto último es lo que da la independencia de hardware. Es equivalente a la máquina virtual de Java.

Figura 2.5.1-1 Componentes de .NET Framework

- La biblioteca de clases .NET o BCL (Base Common Library) que provee un conjunto de clases comunes y de competencia de todos los lenguajes de programación como Visual Basic y C#.

Figura 2.5.1-2- Conjunto de Librería de .NET

- ASP.NET, parte del .NET Framework dedicada al desarrollo web, es la evolución de la tecnología ASP, el .NET en conjunción con el servidor web de Microsoft procesará las aplicaciones desarrolladas con la tecnología ASP.NET.

- ADO.NET, proporciona acceso a datos relacionales, XML y de aplicaciones. Provee componentes para el desarrollo de aplicaciones que manejen bases de datos distribuidas.

- Windows Forms, evolución de la tecnología desarrollada para aplicaciones de escritorio, provee los controles y componentes usados en la generación de formularios.

- Servicios Webs, permiten el intercambio de datos entre aplicaciones de diferentes plataformas utilizando protocolos y estándares. Frecuentemente usado en aplicaciones que "conversan" entre sí a través de Internet. Los 4 principales estándares en servicios webs son: XML, SOAP, UDDI y WSDL. Todos ellos son soportados por .NET.

- La versión más reciente de .NET Framework es la 3.5 que añade nuevas funcionalidades que se pueden visitar en: http://msdn.microsoft.com/en-us/library/bb332048.aspx.

2.5.2 VISUAL BASIC

Lenguaje de programación desarrollado por Microsoft de fácil aprendizaje que integra un entorno de desarrollo (IDE) para programación de todo tipo de aplicaciones como las de escritorio, componentes, servicios webs, ASP y todo lo que se pueda crear y que funciona sobre la plataforma .NET[9].

La versión de Visual Basic que trabajo con la plataforma .NET fue la 7 y se le conoció como Visual Basic .NET, ha habido mejoras en los últimos años, de hecho en Visual Basic 2005 y Visual Basic 2008 las versiones fueron la 8 y la 9 respectivamente. Siendo VB 2008 la última versión del lenguaje. El entorno de desarrollo o IDE es el Visual Studio .NET que es de pago, adicionalmente existe una versión gratuita llamada Visual Basic Express Edition.

Adicionalmente, .NET incorpora librerías para manejo de la criptografía[33].

2.6 METODOLOGIAS DE DESARROLLO

2.6.1 SCRUM

SCRUM fue concebido por los japoneses Hirotaka Takeuchi e Ijukiro Nonaka en 1986 y está orientado a la gestión de proyectos, más que el desarrollo de aplicaciones. Esta metodología tiene un conjunto de prácticas y roles predefinido. El rol principal recae en el Scrum Master que funciona de manera similar a un gestor de proyectos, el Product Owner representa a los usuarios beneficiados (accionistas u otros) y el Team o equipo que incluye a los desarrolladores.

Durante cada sprint (ciclo o iteración), el cual es un período que dura de 15-30 días (determinados por el propio equipo), el equipo crea un software de manera incremental con entregables que son utilizables. El conjunto de características proviene del Product Backlog donde están las funcionalidades priorizadas por iteración.

Todas las funcionalidades que irán en un sprint se discuten en la Sprint Planning Meeting (Reunión de planeamiento del sprint). Durante esta reunión el Product Owner informa al equipo de las funcionalidades que él quiere completar. El equipo determina como se van a comprometer durante el siguiente sprint. Durante el sprint, nadie puede cambiar el Sprint Backlog, es decir los requerimientos están "congelados".

Hay muchas implementaciones de sistemas para realizar a un desarrollo de Scrum. Otros prefieren simplemente una pizarra y anotaciones en un "memo". Una de las principales ventajas de esta metodología es que es muy fácil de aprender y requiere un mínimo esfuerzo para empezar a utilizarla.[24]

2.6.2 XP

También conocida como XP o Programación Extrema, es una metodología de desarrollo ágil creada por Kent Beck[26]. XP establece un conjunto de practicas diarias que deben seguir los involucrados. Estas prácticas que pueden llegar a ser "extremas" con respecto a las formas tradicionales tienen por objetivo desarrollar software de mejor calidad.

Los defensores de las metodologías agiles apuntan a la adaptabilidad que tienen con respecto al cambio de requerimientos en cualquier punto del ciclo de vida del proyecto y busca generar valor de negocio desde la primera entrega.

Los objetivos de XP son los siguientes: Hacer un intento por alinear la productividad y las relaciones humanas, ser un mecanismo para un cambio social, un camino para mejorar, un estilo de desarrollo y disciplina para el desarrollo de software. Pero más allá de eso, el objetivo real es reducir el costo del cambio.

XP determina cuatro actividades dentro del desarrollo de software: Codificar, Depurar, Diseñar y Escuchar. Quizás la más importante aquí es "Escuchar", porque los programadores no conocen probablemente el proceso de negocio, entonces ellos deben estar muy atentos para darle el producto solicitado por los usuarios o clientes. Esto se fortalece si hay un intercambio de información entre el usuario y el programador.

Las prácticas básicas que propone XP son las siguientes:

- **El juego de la planificación**.- Planificación del desarrollo.
- **Integración continua**.- Las modificaciones se añaden al código varias veces durante el día.
- **Semana laboral de 40 horas**.- Solamente se trabaja 40 horas a la semana, en caso de ser necesario un esfuerzo adicional no debe hacerse por mas de 2 semanas.
- **Cliente en el Sitio**.- Esto es un poco difícil, el equipo de desarrollo tiene el tiempo acceso a los involucrados en el proceso de negocio.
- **Estándares de codificación**.- Adopte un estándar para el desarrollo del código.
- **Versiones pequeñas**.- Un sistema sencillo entra pronto en producción. Las funcionalidades se pueden añadir en siguientes iteraciones.
- **Metáfora del sistema**.- Historia que resume el sistema en general y es entendible por todos.
- **Diseño Simple**.- Codifica lo necesario, ni una funcionalidad más.
- **Pruebas continuas**.- Se recomienda desarrollar casos de prueba antes que el codificar la aplicación.

- **Refactorización**.- Buscar mejorar el código existente buscando la reutilización del mismo. Simplificar funciones, mejorar el código de manera constante.
- **Programación en pareja**.- Dos personas trabajan compartiendo una computadora.
- **Posesión grupal del código**.- El código le pertenece a todos y cualquier programador puede cambiar parte del mismo en algún momento.

Existen adicionalmente un esquema de roles, unos formatos de documentación sencillos, complementarios a la información descrita anteriormente. XP está orientado a grupos pequeños, programadores muy buenos y con las actividades en un ambiente en común.

2.6.3 UML

Aunque propiamente no es una metodología, el UML (Unified Modeling Language o Lenguaje unificado de modelado) es un conjunto de diagramas y herramientas que nos permite especificar, visualizar y documentar los modelos de los sistemas de software incluyendo su estructura y diseño.

En 1994, Booch, Rumbaugh y Jacobson dieron forma a la primera versión del UML y en 1997 fue aceptado por la OMG, fecha en la que fue lanzada la versión v1.1 del UML. En la actualidad la última especificación del UML es la 2.1.2.

UML 2.0 está compuesto por un conjunto de diagramas para la modelación de un sistema jerarquizados por funciones y son:

Los Diagramas de Estructura (Structure Diagram) orientados a los elementos que deben existir en el sistema modelado:

- Diagrama de clases.
- Diagrama de componentes.

- Diagrama de objetos.
- Diagrama de despliegue.
- Diagrama de paquetes.
- Diagrama de estructura compuesta .(UML 2.0)

Los Diagramas de Comportamiento (Behavior Diagram) orientados a lo que debe suceder en el sistema modelado:

- Diagrama de actividades.
- Diagrama de casos de uso.
- Diagrama de estados.

Los Diagramas de Interacción (Interaction Diagram) son un subtipo de diagramas de comportamiento, que enfatiza sobre el flujo de control y de datos entre los elementos del sistema modelado:

- Diagrama de secuencia.
- Diagrama de vista de interacción. (UML 2.0)
- Diagrama de colaboración.
- Diagrama de tiempos. (UML 2.0)

2.7 ORGANIZACIONES INVOLUCRADAS

2.7.1 VENTANILLA UNICA DEL ESTADO

Creada por Decreto Supremo Nº019-2007-PCM[34] y apoyado en la Ley Nº27658, Ley Marco de Modernización de la Gestión del Estado y publicada el viernes de 9 de marzo del 2007 en el Diario "El Peruano". Tiene por objetivo de apoyar el mejoramiento de la gestión del Estado impulsando la modernidad,

descentralización y buscando la mayor participación de la ciudadanía teniendo en consecuencia una mejor atención y la optimización de los recursos públicos.

El artículo 1º (Uso de la Ventanilla Única del Estado) dice:

"Establézcase el uso de la Ventanilla Única del Estado a través del Portal de Servicios al Ciudadano y Empresas – PSCE (www.serviciosalciudadano.gob.pe) adscrito al Portal del Estado Peruano – PEP de la Presidencia del Consejo de Ministros como la herramienta a través de la cual se brindan servicios públicos virtuales que ofrezcan las entidades de la Administración Pública.

Todas las entidades de la Administración Pública brindarán sus servicios virtuales mediante la Ventanilla Única del Estado desde la cual podrán vincularse a sus respectivas páginas webs y a los consiguientes servicios que en ella se ofrezcan."

En el siguiente artículo se establece la creación del Sistema Integrado de Servicios Públicos Virtuales SISEV como plataforma que facilitará a la ciudadanía el acceso a los servicios públicos y los relacionados a estos por sectores que se brinden de manera online. El acceso al SISEV se da mediante la Ventanilla Única del Estado (VUE).

La segunda disposición complementaria transitoria de dicho Decreto Supremo establece: "El primer servicio a implementarse bajo la plataforma del Sistema Integrado de Servicios Públicos Virtuales – SISEV será el de constitución de empresas, el mismo que incluirá tanto la inscripción en los Registros Públicos correspondiente como el otorgamiento del número del Registro Único del Contribuyente……".

Asimismo, dicha disposición establece la participación de los Notarios de Lima propuestos por el Colegio de Notarios de Lima.

Figura 2.7.1 Portal de acceso a la Ventanilla Única del Estado

2.7.2 NOTARIAS

Las notarias son instituciones que ejercen función pública y proporcionan a la ciudadanía la seguridad jurídica en el ámbito contractual y extrajudicial por encargo del Estado. Las notarias están bajo responsabilidad del notario, el cual es el profesional con capacidad legal para dar fe pública de los actos en los que interviene.

Entre los principales documentos por legalizar o procesar están los siguientes:

- Constitución de empresas
- Constitución de asociaciones
- Compra Venta de inmuebles
- Constatación de supervivencia
- Entrega de cartas notariales

- Expedición de copias certificadas
- Legalizaciones de Firmas, Libros y/o reproducciones.
- Patrimonio familiar
- Permisos de viaje
- Poderes
- Protesto de Letras
- Sucesiones
- Testamentos
- Otros.

En el departamento de Lima están organizadas bajo el Colegio de Notarios de Lima y para efectos de la iniciativa de la Ventanilla Única del Estado, se consignaron 39 notarías para la participación en dicho proceso.

2.7.3 PROINVERSION

Agencia de Promoción de la Inversión Privada del Perú. Su objetivo principal es promover la inversión no dependiente del Estado Peruano con el fin de impulsar la competitividad del Perú y buscar un desarrollo sostenible logrando así el bienestar de sus ciudadanos.

Sitio Web: http://www.proinversion.gob.pe.

2.7.4 SUNARP

Es la Superintendencia Nacional de los Registros Públicos del Estado Peruano. Tiene por finalidad el otorgamiento de la seguridad jurídica[22] y brindar certidumbre respecto a la titularidad de los derechos que en el se registran y lo concerniente a la función registral en territorio del Perú.

Sitio Web: http://www.sunarp.gob.pe.

2.7.5 SUNAT

Creada bajo el amparo de la Ley Nº24829, la Superintendencia Nacional de Administración Tributaria es una institución pública del sector Economía y Finanzas cuya función principal es la administración, recaudación y fiscalización de los tributos internos del Estado Peruano.

Una de las funciones de la SUNAT es "Celebrar acuerdos y convenios de cooperación técnica y administrativa en materia de su competencia.", que es una función muy relacionada al ámbito de esta tesina. En el sitio web de la SUNAT (http://www.sunat.gob.pe/quienesSomos/funciones.htm), podemos encontrar la lista de las funciones y atribuciones e información adicional.

Sitio Web: http://www.sunat.gob.pe.

PARTE III – ESTADO DEL ARTE

3.1 FIRMA DIGITAL

Una firma digital es un tipo de criptografía asimétrica usada para emular las propiedades de seguridad de una firma escrita a mano en un papel. La firma digital normalmente utiliza dos algoritmos, uno usado para "firmar" la clave privada del usuario y otro para verificar la clave pública del usuario. Una firma provee autenticidad a un mensaje. Los mensajes pueden ser de todo tipo, desde e-mail hasta un contrato.[1]

En la firma digital están involucradas diferentes tecnologías y conceptos como documentos electrónicos, claves criptográficas, certificados digitales, matemáticas, autoridades certificadoras, infraestructura de clave pública y otros que pueden resultarnos desconocidos.

La Firma Digital puede ser aplicada en lo siguiente:

- Correos con autenticidad asegurada
- Contratos comerciales electrónicos
- Transacciones comerciales electrónicas
- Invitaciones electrónicas
- Dinero electrónico
- Notificaciones judiciales electrónicas
- Voto electrónico
- Contratación pública
- y otros tipos de documentación.

3.1.1 TIPOS DE FIRMA DIGITAL

En España, está tipificada bajo la Ley 59/2003[17] los siguientes tipos:

- **Simple.-** Incluye un método de identificar al firmante.
- **Avanzada.-** Además de identificar al firmante permite garantizar la integridad del documento. Se emplean técnicas de PKI (Public Key Infraestructure o Infraestructura de Clave Pública)

- **Reconocida.-** Es la firma avanzada ejecutada con un DSCF (dispositivo seguro de creación de firma) y amparada por un certificado reconocido (certificado que se otorga tras la verificación presencial de la identidad del firmante)

Haciendo un paralelo y en base al artículo 3º de la Ley de Firma Digital, en nuestro país al usarse la tecnología PKI podemos concluir su par con la ley española es la del tipo avanzada.

CARACTERISTICAS LEGALES DE LA FIRMA DIGITAL

- **Autenticidad.**- Determina la identidad del emisor que firma electrónicamente, complementado con el mensaje firmado por éste y al cual se le vincula teniendo de esta manera la certeza que ha sido enviada por dicho emisor.
- **Integridad**.- El mensaje recibido por el receptor es idéntico al enviado por el emisor.
- **No repudio**.- El emisor no puede desconocer el mensaje enviado por él.
- **Confidencialidad**.- El mensaje no puede ser leído por terceras personas que no participan en el proceso de transmisión del mismo.

REQUISITOS IDEALES PARA EL USO DE LA FIRMA DIGITAL

La firma digital tiene varios requerimientos los cuales de no cumplirse afectarian la utilización de dicha tecnología, entre ellos se tiene:

1. **Algoritmos de calidad**.- Se sugiere el uso de algoritmos de clave pública que no sean inseguros, y que no se les haya detectado vulnerabilidades.

2. **Calidad en la implementación**.- Una mala implementación de un buen algoritmo o protocolo podría hacer que no cumpla su función.

3. **La llave privada debe permanecer secreta**.- Si terceras personas llegan a conocerla, dichas personas podrían reproducir la misma firma privada para usos indebidos.

4. **Entrega de las llaves públicas**.- La distribución de las llaves públicas debe ser hecha consiguiendo que la llave de una persona realmente le pertenezca a esa persona. Esto se consigue con la utilización de la infraestructura de clave pública asociada a una autoridad certificadora.

5. Usuarios y el software relacionado debe seguir las reglas y protocolos usados en la firma digital

3.1.2 ¿CÓMO FUNCIONA LA FIRMA DIGITAL?

Las firmas digitales son creadas y verificadas por métodos criptográficos, la función de la matemática aplicada consiste en transformar los mensajes en algo ininteligible y poder regresarlo a su estado original. Las firmas digitales son también conocidas como "criptografía de clave pública" y emplean un algoritmo usando claves matemáticamente diferentes. Una clave sirve para crear una firma digital o transforma la información en algo difícil de entender y la otra clave sirve para verificar una firma digital o retornar el mensaje a su forma original. A esto se le conoce como criptografía asimétrica.

Las claves que se complemente en un sistema de criptografía asimétrica son:

- Clave privada, la cual es solamente conocida por el firmante y es usada para crear la firma digital.

- Clave pública, utilizada para asegurar la entrega y verificación de la firma digital. Si muchas personas necesitan verificar las firmas del emisor o firmantes, la llave pública debe estar disponible o distribuirse a todos, ya sea través de una

publicación en un repositorio en línea o directorio donde sea fácilmente accesible.

A pesar que el par de llaves está matemáticamente relacionado, si el criptosistema asimétrico ha sido bien diseñado e implementado de forma segura es computacionalmente irrealizable derivar la llave privada a partir del conocimiento de la llave pública. Es por esto, que a pesar que muchas personas conocen la clave pública de un firmante y la usan para verificar la identidad del firmante, ellos no pueden descubrir la clave privada del firmante para su propio uso.

Otro proceso fundamental es el llamado "función hash", y es usada en ambas para crear y verificar una firma digital. Una función hash es un algoritmo que crea una representación digital o huella digital bajo la forma de un "valor hash" o "resultado hash" de una longitud estándar el cual es usualmente mucho más pequeño que el mensaje pero que es un valor único.

Cualquier cambio en el mensaje produce un valor hash diferente al del generado por el mensaje original. Adicionalmente es también computacionalmente irrealizable derivar el mensaje enviado conociendo el resultado de la función hash. Las funciones hash en consecuencia posibilitan la creación de firmas digitales que operan con poca utilización de datos. Esto último le añade robustez al sistema pues asegura que el mensaje no ha recibido modificación alguna desde que fue firmado digitalmente.

En consecuencia, tenemos que el uso de las firmas digitales involucra dos procesos, uno realizado por el firmante y el otro por el receptor de la firma digital:

Creación de la firma digital, usando un resultado hash derivado y único, tanto para el mensaje firmado y una clave privada. Por el resultado hash que sea seguro, debe haber sólo una parte insignificante posibilidad de que la misma firma digital puede ser creada por la combinación de cualquier otro mensaje o clave privada.

Verificación de la firma digital, proceso de chequeo de la firma digital por referencia con el mensaje original y dado una clave pública.

Típicamente una firma digital es adjuntada a su mensaje y se almacena o se transmite sin el. Sin embargo, puede que sea almacenada como un documento separado, tanto como se mantenga la correspondencia con el mensaje.

3.1.4 PKI - INFRAESTRUCTURA DE CLAVE PÚBLICA

Derivada del acrónimo inglés "Public Key Infrastructure" es una combinación de tecnologías a nivel físico (hardware) y de aplicaciones (software), reforzada con políticas y procedimientos de seguridad que posibilitan la ejecución de las operaciones criptográficas con garantía como es el caso de la firma digital o el no repudio de transacciones electrónicas.

PKI involucra todos los entes participantes en el proceso de criptografía asimétrica en comunicaciones electrónicas como por ejemplo la autoridad certificadora o de certificación.

Basándose en la criptografía asimétrica, la PKI emplea en el proceso la figura de la clave privada y pública, la primera para cifrar y la segunda para descifrar.

El objetivo primordial de la infraestructura PKI es la de asegurar las transacciones electrónicas en su dominio o entorno proveyendo claves y gestionando los certificados confiables logrando así las conocidas garantías de autenticación, confidencialidad y no repudio. Esta infraestructura se suele ver de forma frecuente en Internet protegiendo las transacciones que en la red se realizan.

La implementación funcional de PKI posibilita entregar al menos los siguientes servicios:

- Servicios de Certificación: Garantías de autenticidad, confidencialidad e integridad de los datos a través de una plataforma de certificación, gestión de usuarios, control de revocados y otros.

- Servicios de certificación temporal y timbre digital.
- Disponer de un conjunto homogéneo y compatible de soluciones criptográficas.
- Asesoramiento y apoyo en cuanto a soluciones disponibles ante problemas que surjan en la implementación de otros proyectos.

Componentes Principales de PKI

Entre los componentes que interactúa o interrelacionan en la infraestructura de PKI tenemos:

- Una Autoridad de Certificación
- Certificados Digitales y listas de Revocación
- Pares de claves matemáticamente relacionadas, disponiendo en cada par de una clave privada y una clave pública Tales elementos se desarrollan dentro de una estructura formal determinada por:
- Políticas de Certificación
- Manuales de Procedimientos

Una Autoridad de Certificación (AC) es la organización responsable de la emisión de los certificados, luego de una correcta verificación por los métodos que considere en la política de certificación. Adicionalmente, representa al usuario que ha sido reconocido por el resto en un determinado entorno como certificador de las identidades digitales de todos.

Una AC es el principal proveedor de la tecnología de criptografía asimétrica. Debe contar con medidas de seguridad que infundan la total confianza requerida para considerara a su gestión seria y exitosa y ostentar altos niveles de calidad en la prestación y disponibilidad de sus servicios.

La función principal de una Autoridad de Certificación es la de verificar la identidad de los solicitantes de certificados, crear los certificados digitales y publicar listas de revocación cuando éstos son desechados.

Una Autoridad de Certificación se puede identificar[29]:

- Por organización: la autoridad certificante emite certificados a individuos afiliados a una organización.
- Por residencia: emite certificados a individuos basándose en una dirección geográfica. Desde el punto de vista gubernamental podría decirse que asumen la responsabilidad por estos certificados en debido estado.
- Por persona: es un caso especial donde la certificación no reclama la inserción de su nombre en el certificado con una persona física o entidad. Está establecido para acomodar a usuarios que desean encubrir su identidad cuando hacen uso de las facilidades de seguridad.

Una Autoridad de Certificación puede valerse para sus funciones del apoyo de Autoridades de Registro (AR) cuya misión es verificar la autenticidad de las personas naturales o jurídicas (validación de identidad) que requieren la emisión de un certificado y realizar la solicitud formal pertinente (Registro de presentaciones).

Esta interacción entre ACs y ARs permite expandir y descentralizar el proceso de certificación, pues las ACs sólo aceptan a las personas identificadas a las ARs de cada región.

Las Políticas de Certificación y los Manuales de Procedimiento definen cuestiones tan esenciales como el tipo de certificado a emitir por la Autoridad de Certificación, el alcance de la información almacenada en el certificado, los procedimientos de registro, el tipo y alcance del compromiso de la Autoridad de Certificación con los usuarios y viceversa, las restricciones en el uso del certificado, etc. Además, al momento de crear el certificado digital este debe cumplir con las leyes asociadas y vigentes. El valor legal de una firma digital validada con un certificado calificado dependerá fuertemente de la política que gobierna el uso de la clave privada asociada.

La publicación de certificados y de las listas de revocación de los mismos debe ser publicada en un directorio, los usuarios de la PKI deben tener acceso para la comprobación de firmas. Además, se le debe prestar atención a la no publicación de

datos sensibles. Muchas veces puede convertirse en un elemento crítico si no se le presta la debida atención.

Complementariamente a la Autoridad de Certificación también se presentan las siguientes organizaciones[29]:

- **Autoridades Certificantes Licenciadas:** Son aquellos organismos o dependencias que soliciten y obtengan la autorización, por parte del Organismo Licenciante, para actuar como Autoridades Certificantes de sus propios agentes.
- **Organismo Licenciante:** Es la Autoridad Certificante Raíz que emite certificados de clave pública a favor de aquellos organismos o dependencias que deseen actuar como Autoridades Certificantes Licenciadas, es decir como emisores de certificados de clave pública para sus funcionarios y agentes.
- **Organismos Auditantes:** Es el órgano de control, tanto para el Organismo Licenciante como para las Autoridades Certificantes Licenciadas.

3.1.5 CERTIFICADOS DIGITALES

Un certificado digital es un documento digital que garantiza el vínculo entre un individuo u organización y su clave pública. Este certificado es emitido por una Autoridad de Certificación (CA).

Entre todos los campos contenidos en un certificado digital, los más significativos son:

- Una clave pública asociada al dueño del certificado
- El nombre distintivo del dueño del certificado
- Una fecha de expiración
- El nombre de la Autoridad de Certificación emisora
- Un número de serie
- Firma de la Autoridad de Certificación emisora
- Información opcional

El más utilizado en la actualidad es el basado en el estándar UIT-T X.509. También conocido como X.509, es la pieza central de la infraestructura de clave pública y es la estructura de datos que enlaza la clave pública con los datos que permiten identificar al titular. Este certificado posee la siguiente estructura:

- Versión
- Número de serie
- ID del algoritmo
- Emisor
- Validez (No antes de, No después de)
- Sujeto
- Información de clave pública del sujeto (Algoritmo de clave pública, Clave pública del sujeto)
- Identificador único de emisor (opcional)
- Identificador único de sujeto (opcional)
- Extensiones (opcional)
- Otros
- Algoritmo usado para firmar el certificado
- Firma digital del certificado

CAs en Perú

En Perú la Entidad de Certificación Nacional para el Estado Peruano, que cumple funciones de Entidad de Registro y Verificación es:

- Registro Nacional de Identificación y Estado Civil RENIEC

En Perú la Autoridad Administrativa Competente de la Infraestructura Oficial de Firma Electrónica es:

- Instituto Nacional de Defensa de la Competencia y de la Propiedad Intelectual INDECOPI

3.1.6 TARJETAS INTELIGENTES (SMART CARDS)

Una Smart Card o tarjeta inteligente es un dispositivo que incorpora un circuito integrado que puedes ser un microcontrolador seguro o equivalente inteligente con memoria interna o un chip de memoria solamente. La tarjeta se conecta a un lector de forma directa (física) o con una interfaz de radio frecuencia que no necesita contacto. Cuando tienen un microcontrolador, las smart cards pueden almacenar grandes capacidades de información además de las propias funciones de la tarjeta. Un ejemplo de esto es la encriptación y autenticación de datos) e interactúa de manera inteligente con el lector respectivo (Smart Card Reader)[30].

La tecnología de tarjetas inteligentes sigue estándares internacionales como el ISO/IEC 7816 y ISO/IEC 14443 y tiene múltiples presentaciones como tarjetas plásticas, llaveros, relojes, tokens USB y otros. Como mecanismo de control de acceso las tarjetas inteligentes hacen que los datos personales y de negocios solo sean accesibles a los usuarios apropiados, esta tarjeta asegura la portabilidad, seguridad y confiabilidad en los datos.

La incorporación de un circuito integrado ofrece tres nuevos elementos que pueden favorecer su utilización generalizada:

Miniaturización: La alta densidad de circuitos integrados y otros componentes en un área pequeña, permite ofrecer un nuevo abanico de posibilidades y de funciones, lo que origina su expansión en el mercado y un nuevo medio de intercambio de información.

Lógica programable: La Smart Card, incorpora funciones lógicas de programación como una computadora.

Interfaz directa de comunicaciones electrónicas: Las comunicaciones están en crecimiento constante. Cada nuevo avance ofrece un nuevo campo en el que puede aplicarse las tarjetas inteligentes. Las especificaciones físicas, eléctricas, el formato de los comandos y todo lo relacionado con tarjetas se especifica en la norma ISO 7816

Utiliza clave de acceso o PIN: Para poder utilizarse es necesario digitar un número de identificación personal, es posible además incorporar tecnología más avanzada como identificación por técnica biométrica, huella digital o lectura de retina.

Para el caso de la aplicación de encriptación desarrollada se está usando el tipo de tarjeta inteligente Smart Card Reader LTC31

3.1.7 LLAVES ETOKEN

eToken es una herramienta USB de administración de contraseñas y llaves criptográficas. Sirve para usarse en la generación y almacenamiento seguro de contraseñas, certificados digitales, autenticación fuerte segura, firmas digitales y encriptación.

eToken proporciona seguridad a los datos con base en la tecnología Smartcard y sin requerir lectores especiales. Proporciona un conjunto de soluciones listas para usarse para el control de la seguridad y acceso a la red de computadoras cubriendo todas las necesidades de autenticación (acceso vía web, acceso vía VPN y acceso a la red) y proporciona seguridad de archivos y de laptops.

Además de ayudar a administrar y almacenar contraseñas, eToken asegura la autenticación fuerte de doble factor del usuario, ayuda a proteger contra el

phishing y otros intentos no autorizados de acceso, hace posible la implementación del acceso remoto a través de identificación por medio de foto y refuerza la seguridad de la PC.

La asignación, distribución y personalización del eToken dentro de una organización son administradas de forma fácil a través del Token Management System (TMS), basado en Active Directory.

3.2 MARCO LEGAL DE LA FIRMA DIGITAL EN EL PERU

El Estado Peruano ha promovido las siguientes leyes en referentes al campo de la Firma digital.

- Ley de Firmas y Certificados Digitales. Ley Nº 27269. (Año 2000)

- Ley que modifica el Artículo 11° de la Ley N° 27269. Ley Nº 27310. (Año 2001)

- Reglamento de la Ley de Firmas y Certificados Digitales. DS Nº 019-2002-JUS (Año 2002).

- Disposiciones Complementarias al Reglamento de la Ley de Firmas y Certificados Digitales. Nº 0103-2003/CRT-INDECOPI (Año 2003)

- Ley que dispone la recaudación de un aporte por supervisión y control anual por parte del INDECOPI de las entidades de certificación y de verificación/registro de firmas digitales acreditadas bajo su ámbito. Ley Nº 28403. (Año 2004)

- Nuevo Reglamento de la Ley de las Firmas y Certificados Digitales. D.S N° 004-2007-PCM. (Año 2007)

Respecto a las leyes podemos comentar que la Autoridad de Certificación o Prestador de Servicios de Certificación en nuestro país es la INDECOPI establecida

en el Reglamento de la Ley de las Firmas y Certificados Digitales. Asimismo, la que la ley 27730 al modificar el artículo 11 le dio validez y eficacia jurídica a los certificados emitidos por las autoridades extranjeras siempre y cuando sean reconocidos por la autoridad administrativa competente.

PARTE IV - DESARROLLO DE LA SOLUCION

4.1 AMBITO DE LA SOLUCION

4.1.2 PARTICIPACION DE LOS ORGANISMOS

Las coordinaciones con las instituciones participantes en este proceso se da desde Octubre del 2004 con la creación de Centro de Desarrollo de Nuevas Tecnologías – CEDETEC – en el Colegio de Notarios de Lima. Por esa misma fecha de da el Acuerdo con el Consejo del Notariado Español y se firma un contrato de tercerización con la Agencia Notarial de Certificación – ANCERT – para incorporar las firmas y certificados digitales en la actividad notarial.

A comienzo del 2006 (Enero de ese ano), el Colegio de Notario de Lima (CNL) y la Superintendencia Nacional de Registros Públicos (SUNARP) firman un convenio para la presentación de documentos por vía electrónica. En Junio de las 2006 ambas instituciones (CNL y SUNARP) se incorporan al plan piloto de la Oficina de Gobierno Electrónico para el desarrollo de servicios en el portal de servicios del ciudadano.

Para poder realizar esta incorporación en el Portal de servicios de ciudadano se incorporan procesos de la SUNAT en la generación, expedición y entrega del RUC. También se incluyeron proceso RENIEC para la validación de la identidad de las personas a través del ingreso de número de DNI

Tanto el Programa Mi Empresa así como PROINVERSION, se encargarían de la difusión y capacitación del uso de este nuevo proceso de Constitución de Empresas en Línea

De acuerdo a esto antecedentes, las instituciones participantes en el Proceso de Constitución de Empresas en Línea son:

- Presidencia de Consejo de Ministros, a través de la Oficina Nacional de Gobierno Electrónico (ONGEI).

- Colegio de Notarios de Lima, a través del CEDETEC.
- Superintendencia Nacional de Registros Públicos (SUNARP).
- Superintendencia de Administración Tributaria (SUNAT).
- Registro Nacional de Identificación y Estado Civil (RENIEC).
- Programa Mi Empresa.
- Agencia de Promoción de la Inversión Privada (PROINVERSION).

Examinando el aporte que tendrá cada institución nombrada y los procesos inherentes a cada una de ellas y teniendo en cuenta el apoyo tecnológico de cada uno de los participantes el proyecto funcionara de la siguiente manera:

Portal de Servicios al Ciudadano y Empresas

Ofrecer a los ciudadanos y público en general una ventanilla única de trámites y servicio del Estado.

Medio de Pago Virtual

Implementar mecanismos de pagos en línea

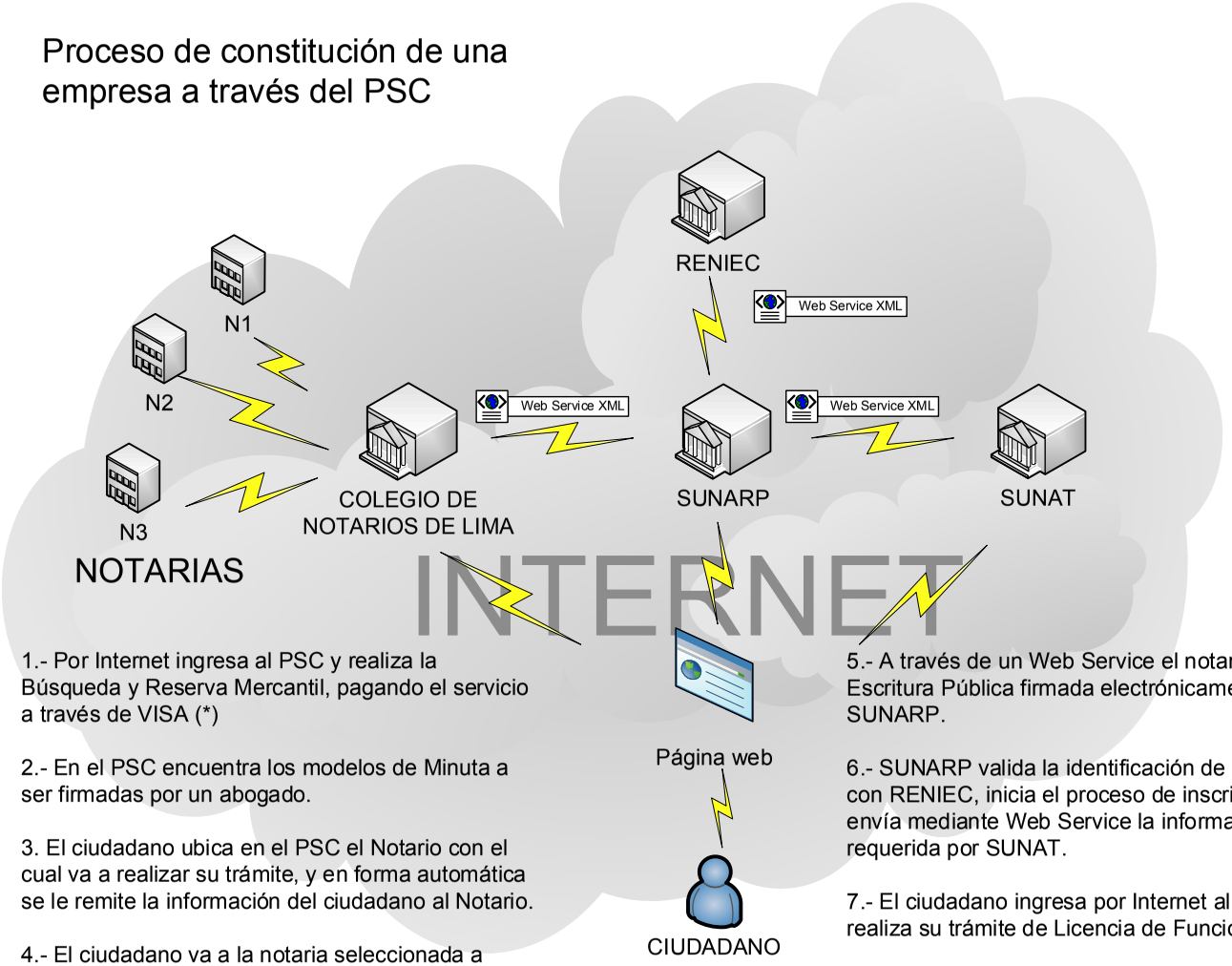
Firma Digital

Brindar la seguridad respectiva y el no repudio a las transacciones de Internet.

Red Transaccional del Estado

Tendrá a su cargo la Integración e Iteración de la información de las diferentes instituciones participantes del Estado utilizando Web Services vía Internet.

Proceso de constitución de una empresa a través del PSC



1.- Por Internet ingresa al PSC y realiza la Búsqueda y Reserva Mercantil, pagando el servicio a través de VISA (*)

2.- En el PSC encuentra los modelos de Minuta a ser firmadas por un abogado.

3. El ciudadano ubica en el PSC el Notario con el cual va a realizar su trámite, y en forma automática se le remite la información del ciudadano al Notario.

4.- El ciudadano va a la notaria seleccionada a firmar la Escritura Pública.

5.- A través de un Web Service el notario envía la Escritura Pública firmada electrónicamente a SUNARP.

6.- SUNARP valida la identificación de las personas con RENIEC, inicia el proceso de inscripción y envía mediante Web Service la información requerida por SUNAT.

7.- El ciudadano ingresa por Internet al PSC y realiza su trámite de Licencia de Funcionamiento.

El sistema consiste en una reducción de los pasos a seguir que actualmente se realizan para poder constituir una Mype, realizándose estos en línea ingresando desde cualquier lugar (hogar, oficina, cabina pública, etc.) al portal de servicios al ciudadano www.serviciosalciudadano.gob.pe, o a través de las notarías o de un asesor en las oficinas de Mi Empresa del Ministerio de Trabajo y Promoción del Empleo.

Luego de ingresar al portal mencionado, realiza los siguientes pasos:

El solicitante, después de verificar razón social elegida para su empresa en SUNARP, accede al portal de servicios al ciudadano, selecciona una notaría de la lista en donde se presentará y escoge un modelo de constitución de empresas validado por SUNARP (o remite uno de sus propios modelo).

El Notario, con esta información y luego de emitir una constancia para apertura de cuenta en el banco y de recibir la constancia bancaria del depósito, prepara la escritura con los datos recibidos electrónicamente desde el portal.

El solicitante abre una cuenta corriente en el banco y con dicho numero, acude a la notaria a firmar la escritura pública. El Notario, conforme a ley, da fe de la identidad, capacidad, libertad y conocimiento de los otorgantes y valida en línea con RENIEC la identidad del representante legal. Luego se firma la escritura pública ante el Notario y este prepara el parte. El solicitante podrá pagar los derechos registrales desde la misma notaría.

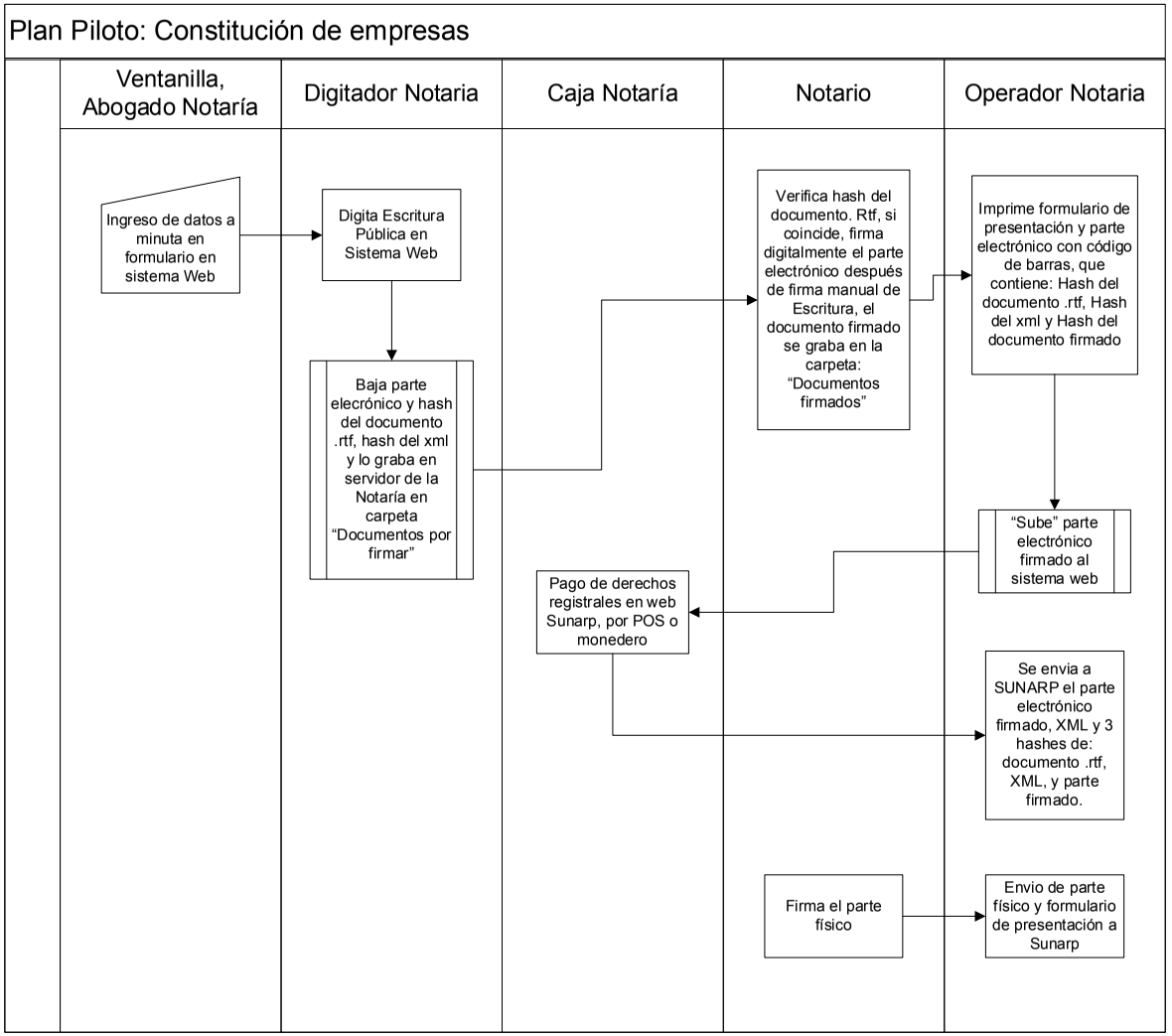
Luego, el Notario remite parte electrónico con firma digital a SUNARP y el parte físico de respaldo con el código de encriptación. SUNARP recibe el parte electrónico y lo compara con el físico. Califica el parte electrónico y lo inscribe.

SUNARP solicita en línea (Web Service) a SUNAT la generación del número de RUC, quien lo realiza electrónicamente y responde por la misma vía.

SUNARP emite en su portal la constancia de inscripción que contiene el número de RUC y lo remite al Notario por vía electrónica quedando realizada la inscripción conforme a ley.

Finalmente, el representante legal o solicitante recoge en la misma Notaria el testimonio con la constancia de inscripción, el RUC asignado y la Clave SOL quedando así constituida ya su empresa.

Adicionalmente al grafico del proceso descrito, presentamos el flujo de datos propuestos de la Constitución de Empresas en Línea: (Ver Gráfico en la siguiente Hoja)


Plan Piloto: Constitución de empresas
Ventanilla, Abogado Notaría
Digitador Notaria
Caja Notaría
Notario
Operador Notaria
Ingreso de datos a minuta en formulario en sistema Web
Digita Escritura Pública en Sistema Web
Baja parte elecrónico y hash del documento .rtf, hash del xml y lo graba en servidor de la Notaría en carpeta "Documentos por firmar"
Pago de derechos registrales en web Sunarp, por POS o monedero
Verifica hash del documento. Rtf, si coincide, firma digitalmente el parte electrónico después de firma manual de Escritura, el documento firmado se graba en la carpeta: "Documentos firmados"
Firma el parte físico
Imprime formulario de presentación y parte electrónico con código de barras, que contiene: Hash del documento .rtf, Hash del xml y Hash del documento firmado
"Sube" parte electrónico firmado al sistema web
Se envia a SUNARP el parte electrónico firmado, XML y 3 hashes de: documento .rtf, XML, y parte firmado.
Envio de parte físico y formulario de presentación a Sunarp

Con estos procesos modificados el trámite se realiza en un tiempo máximo de tres días hábiles ya que casi todos los procesos se realizan en línea, el solicitante tiene una presencia física mínima, se puede realizar el seguimiento en línea, no necesita minuta, solo se consigna información al inicio, se obtiene la entrega de RUC y clave SOL y se reduce errores en digitación.

Asimismo, se minimiza la falsificación y adulteración de documentos, se minimiza costos asociados a abogados, tramitadores, transportes, etc; se reduce costos notariales por estandarización de formatos y también se disminuye las operaciones registrales por uso de formatos pre aprobados.

4.2 ARQUITECTURA DEL SISTEMA

Mediante el proyecto se considera que para realizar los procesos de constitución de empresas, el ciudadano solo tenga que desplazarse a un solo lugar para completar con los requerimientos de todas las instituciones participantes, permitiendo asimismo monitorear el estado del trámite desde Internet ingresando al Portal de Servicios al Ciudadano y Empresas.

Portal de Servicios al Ciudadano y Empresa (PSCE):

El ciudadano podrá encontrar en el PSCE la ventanilla única de trámites y servicios con el Estado, y podrá hacer el seguimiento a sus trámites y servicios. Se ha implementado el uso de un número secreto de identificación personal que será almacenado por el RENIEC y formará parte del registro de identidad.

Búsqueda y Reserva Mercantil:

Vía Internet se registrara en el Portal de Servicio al Ciudadano y de manera electrónica se realizará la búsqueda de la razón social y la reserva mercantil en caso de no encontrarse en los registros de datos de la SUNARP.

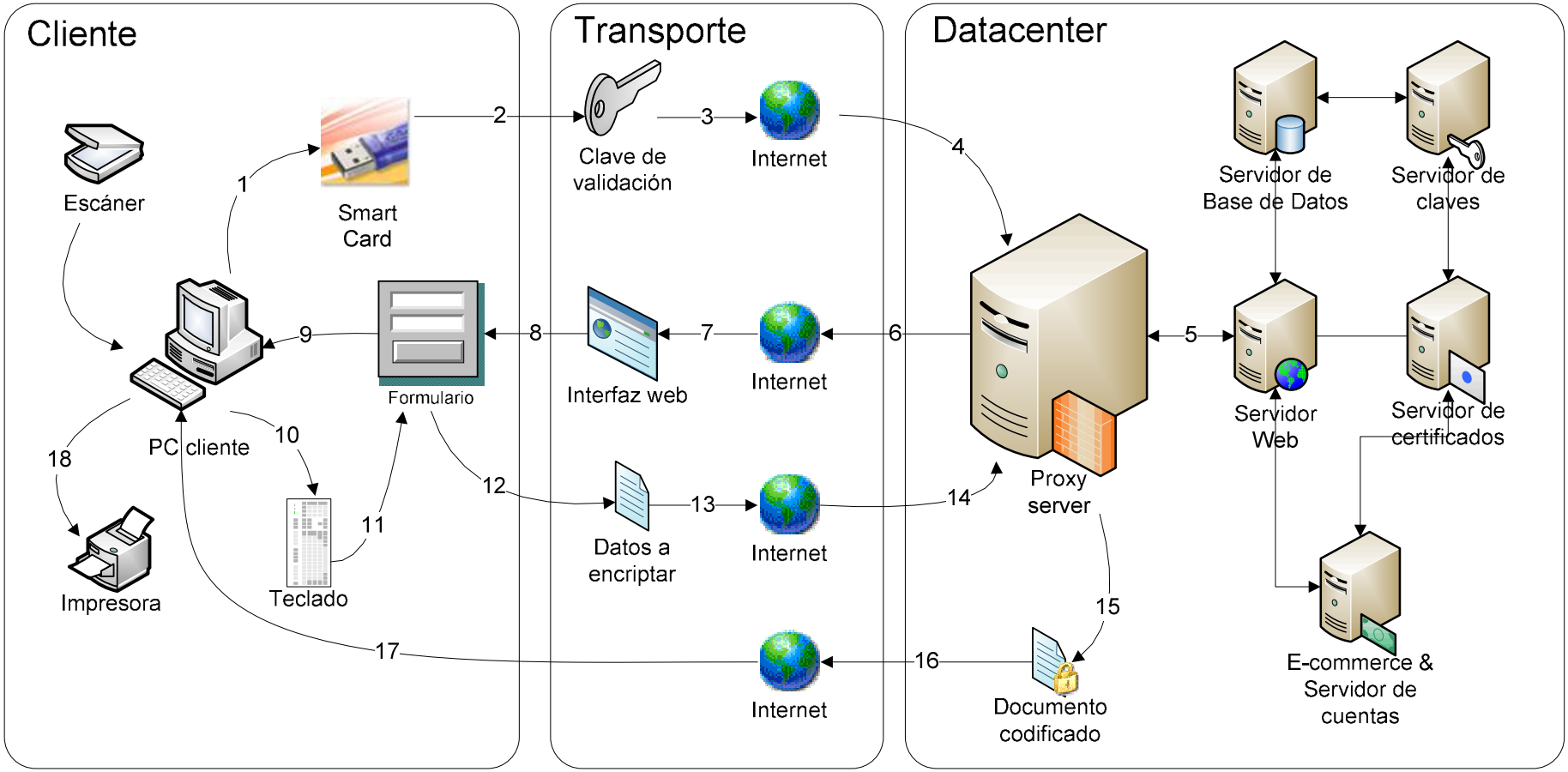
Redacción de la Minuta:

Los solicitantes podrán encontrar en el PSCE los Modelos de Minuta aprobados por el Colegio de Notarios y La SUNARP.

Elaboración de la Escritura Pública, Inscripción de la Empresa - SUNARP y Registro Único del Contribuyente – SUNAT:

Se logra la interacción entre los organismos públicos involucrados. Con esto se busca que el ciudadano solo tendrá que ir en forma física a cualquier notaría para la obtención de la Escritura Pública y el RUC, adicionalmente en la notaría se pagará los servicios notariales y la inscripción en la SUNARP, centralizando de esta manera el pago por los diferentes servicios.

Arquitectura del sistema



4.3 DESCRIPCION DE LA SOLUCION

La solución propuesta en este capítulo solo tomará la opción de encriptación y lectura de documentos ya que para la solución general señalada se necesita de la intervención de diferentes organismos del Estado y de la sinergia de los mismo así como la voluntad política para llevarla acabo.

El sistema que se propone es el Sistema de Protección de Archivos de Constitución de Empresas, no contempla estructuras de base de datos por no ser necesarias para la demostración de la aplicación, la cual si será usada en el desarrollo general tal como se muestra en los gráficos del presente capitulo.

En esta sección se presenta la funcionalidad del Sistema de Protección de Archivos de Constitución de Empresas, así como los prototipos que se han desarrollado para las aplicaciones Encriptador y Verificador de la solución propuesta.

4.3.1 ENCRIPTADOR

El Encriptador es la aplicación que permite manejar un repositorio seguro de archivos, protegiendo la integridad de éstos mediante la encriptación de su contenido bajo el esquema de firma digital.

Así mismo permite la impresión de cada documento incorporándole un contenedor digital en formato análogo (papel) en donde encripta una sumilla de datos que identifican al documento y mediante los cuales éste puede ser verificado con su contraparte digital.

4.3.2 VERIFICADOR

El Verificador es la aplicación que permite corroborar la integridad y la autoría del documento electrónico (archivo BIN), que fue generado por el Encriptador, versus el documento impreso con el código esteganográfico.

Esta verificación se realiza mediante el escaneo del código esteganográfico (del cual se obtienen los datos encriptados previamente) y la comparación del dato HASH extraído del código contra el HASH calculado del archivo BIN.

4.4 DIAGRAMAS UML

En esta sección se presenta el análisis realizado para la presente solución haciendo uso de la metodología RUP con modelamiento UML, de la cual se obtienen los modelos que se muestran a continuación.

Modelo de Casos de Uso de Negocios (Business Use-Case Model)

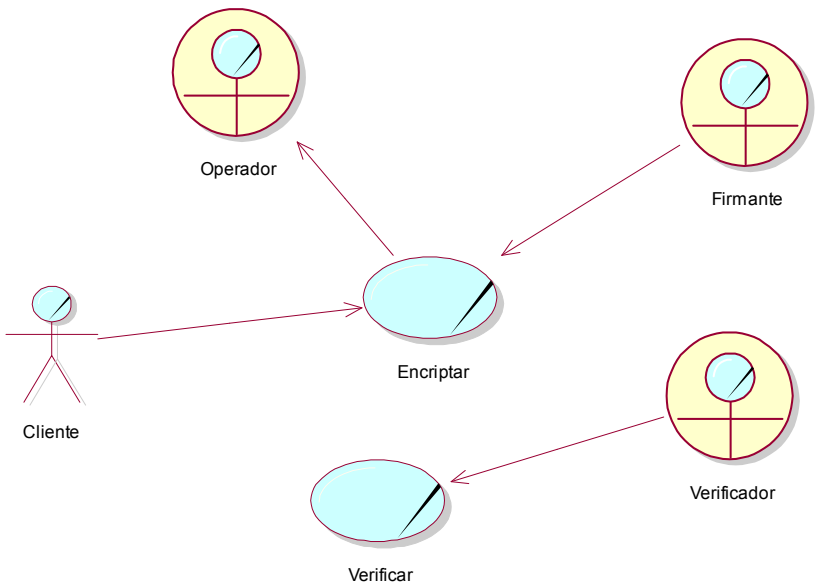
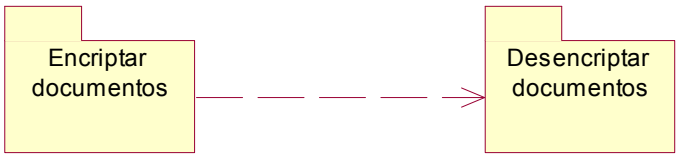
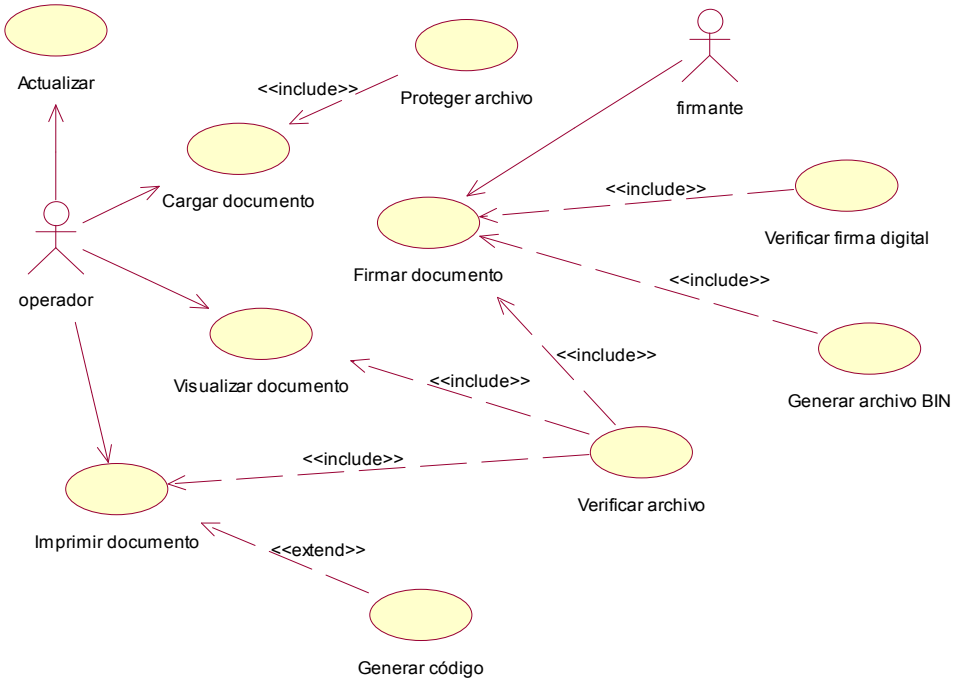


Diagrama de Paquetes

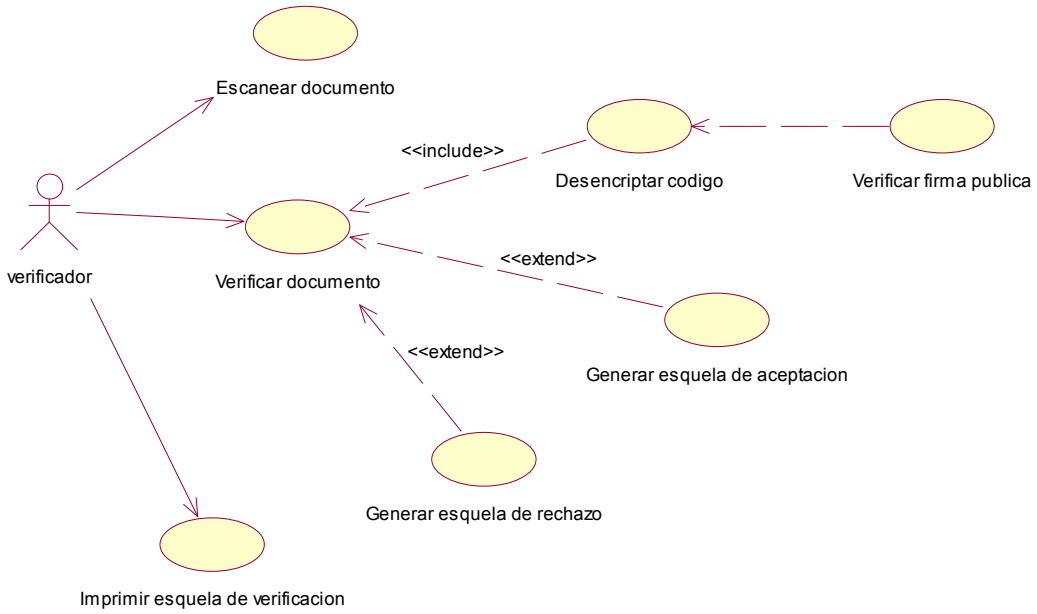


Modelo de Casos de Uso (Use Case Model)

Encriptar Documentos:



Desencriptar Documentos:



CASOS DE PRUEBA

CASOS DE PRUEBA: APLICACION ENCRIPTADOR

Caso de Prueba: 1	**Opción : Nuevo**	**Módulo : Encriptación de Documentos**	**Estado del caso: APROBADO**
Requisitos de Prueba: Ninguno			
Objetivo del Caso de Prueba: Poner en blanco lo valores de la grilla.			

Paso	**Instrucción**	**Resultados Esperados**	**Observaciones / Comentarios**
1	Ingresar al sistema Encriptación de Documentos, seleccionar la opción de Nuevo.	Se mostrará una pantalla con los datos que contiene la grilla en ese momento.	
2	Hacer clic en el botón Nuevo	La funcionalidad de este proceso es permitir al usuario cargar un nuevo documento dentro del repositorio seguro del Sistema de Protección de Archivos Se mostrará la opción “Cargar Nuevo Zip” en la sección de detalle de procesos de la aplicación. Haciendo clic en el botón “Buscar”, seleccionamos la ruta desde donde se van cargar los archivos de formato **.zip.** Confirmado el archivo que será cargado la aplicación internamente realiza el proceso de descompresión de archivo zip y procede a proteger los archivos, cifrándolos y haciendo uso de la firma digital propietaria de la aplicación.	

Caso de Prueba: 2	Opción : Actualizar	Módulo : Encriptación de Documentos	Estado del caso: APROBADO
Requisitos de Prueba: Ninguna			
Objetivo del Caso de Prueba: Buscar archivos a encriptar.			

Paso	Instrucción	Resultados Esperados	Observaciones / Comentarios
1	Ingresar al sistema Encriptación de Documentos, seleccionar la opción de Actualizar.	Se mostrará una pantalla con una grilla de datos La grilla de datos, contendrá los campos de Notaria, Kardex, Fecha/hora y Estado	
2	Hacer clic en el botón Actualizar.	La funcionalidad que se cumple aquí es la de Refrescar la pantalla, recorriendo la carpeta o repositorio de la aplicación para cargar en la grilla los nuevos archivos pendientes en estado **Por Firmar** o **Por Imprimir**. En la sección de detalle de procesos de la aplicación podemos observar los datos del documento seleccionado.	

Caso de Prueba: 3	Opción : Visualizar	Módulo : Encriptación de Documentos	Estado del caso: APROBADO
Requisitos de Prueba: Ninguna			
Objetivo del Caso de Prueba: Visualizar archivos a encriptar.			

Paso	Instrucción	Resultados Esperados	Observaciones / Comentarios
1	Ingresar al sistema Encriptación de Documentos, seleccionar la opción de Actualizar.	Se mostrará una pantalla con una grilla de datos	
2	Hacer clic en el botón Visualizar.	Aquí podemos visualizar los documentos que se encuentren en los estados Por Firmar, Por Imprimir mostrados en la bandeja de Pendientes, o estado Cerrado que se encuentran en la bandeja de Históricos. En la sección de detalle de procesos de la aplicación contamos con el botón de "Visualizar Documento" que nos permite abrir una ventana en la que se pre-visualiza el contenido del documento.	

Caso de Prueba: 4	Opción : Firmar	Módulo : Encriptación de Documentos	Estado del caso: APROBADO
Requisitos de Prueba: Ninguna			
Objetivo del Caso de Prueba: Se obtiene la firma con que encriptar el documento.			

Paso	Instrucción	Resultados Esperados	Observaciones / Comentarios
1	Ingresar al sistema Encriptación de Documentos, seleccionar la opción de Actualizar.	Se mostrará una pantalla con una grilla de datos	
2	Hacer clic en el botón Firmar.	Hacemos clic en el botón “Firmar” e inmediatamente se cargará una ventana solicitando ingresar el PIN o código secreto de la Autoridad Firmante. Para esto se debe contar con el Smart Card y la tarjeta chip de memoria protegida que contiene la Firma Digital de la Autoridad Firmante. En seguida de ingresado el PIN, se carga la ventana en la que se seleccionará la ruta donde se generará el archivo de tipo BIN que es el “Archivo ya Firmado”. Hacemos clic en botón “OK” y con esto estamos encriptando el documento con la Firma Digital Privada del Notario obtenida del dispositivo externo SMART CARD. El archivo generado en este proceso (extensión BIN) es el que se enviará electrónicamente al Organismo Receptor del documento. Una vez firmado digitalmente el documento se muestra un mensaje de confirmación, en el que nos indica que se generó el archivo correctamente	

Caso de Prueba: 5	Opción : Imprimir	Módulo : Encriptación de Documentos	Estado del caso: APROBADO
Requisitos de Prueba: Ninguna			
Objetivo del Caso de Prueba: Imprimir el documento con el código de encripcion como parte oficial o sin el cómo borrador.			

Paso	Instrucción	Resultados Esperados	Observaciones / Comentarios
1	Ingresar al sistema Encriptación de Documentos, seleccionar la opción de Actualizar.	Se mostrará una pantalla con una grilla de datos La grilla de datos, contendrá los campos de Notaria, Kardex, Fecha/hora y Estado	
2	Hacer clic en el botón Imprimir.	En este proceso solo permite imprimir los documentos que ya han sido firmados así que en caso de seleccionar un registro que no cumpla con dicha validación se mostrará el mensaje de error correspondiente. Funcionalmente este proceso tiene dos opciones de impresión que describimos a continuación: Imprimir Parte Borrador: permite imprimir el documento RTF original sin el código esteganográfico. Imprimir Parte Oficial: permite imprimir el documento RTF original con el Contenedor Digital Análogo (Código Esteganográfico), el cual solo será generado sólo si han sido instalados los certificados digitales correspondientes a las firmas propietarias de la aplicación EntersysSender y EntersysReceiver. Dicho código encriptará e incluirá en él los datos obtenidos de la sumilla (archivo TXT) en donde incrusta el hash del documento digital que será usado para la validación del documento en el organismo receptor.	

CASOS DE PRUEBA: APLICACION VERIFICACION

Caso de Prueba: 1	**Opción : Seleccionar Scanner**	**Módulo : Verificación de Documentos**	**Estado del caso: APROBADO**
Requisitos de Prueba: Ninguno			
Objetivo del Caso de Prueba: Selecciona el Scanner disponible en el sistema			

Paso	**Instrucción**	**Resultados Esperados**	**Observaciones / Comentarios**
1	Ingresar al sistema Verificación de Documentos, seleccionar la opción de Seleccionar.	Se mostrará una pantalla con los datos que contiene la grilla en ese momento.	
2	Hacer clic en el botón Seleccionar Scanner	Este proceso nos permitirá seleccionar el dispositivo externo mediante el cual se realizará el proceso de escaneo del documento.	

Caso de Prueba: 2	Opción : Actualizar	Módulo : Verificación de Documentos	Estado del caso: APROBADO
Requisitos de Prueba: Ninguna			
Objetivo del Caso de Prueba: Scannear documento a ser verificado.			

Paso	Instrucción	Resultados Esperados	Observaciones / Comentarios
1	Ingresar al sistema Verificación de Documentos, seleccionar la opción de Scannear.	Se mostrará una pantalla con una grilla de datos	
2	Hacer clic en el botón Scannear.	Este proceso nos permitirá la digitalización de los datos contenidos en el código esteganográfico mediante los cuales de verificará la validez del documento digital a través de la comparación de hashes. El primer paso para este proceso es seleccionar el archivo BIN que será objeto de verificación, para esto hacemos clic en el botón Browse e inmediatamente aparecerá un cuadro de dialogo en donde podemos indicar la ruta del archivo. Una vez cargado el archivo procedemos a colocar en el escáner una de las hojas del documento impreso y hacemos clic en el botón “Escanear”. Seleccionamos la región del código esteganográfico y hacemos clic en el botón Scan. La aplicación procederá a digitalizar y decriptar el código (previa verificación de la existencia de los certificados de la firma digital correspondientes, un público y un privado por ser cifrado asimétrico) para luego obtener los datos ocultos que permitirán obtener el campo llave (hash) con el cual hará el match con el archivo BIN precargado. Si el match es correcto mostrará un mensaje de verificación completada. Luego procede a mostrar los datos descifrados en pantalla	

Caso de Prueba: 3	Opción : Imprimir	Módulo : Verificación de Documentos	Estado del caso: APROBADO
Requisitos de Prueba: Ninguna			
Objetivo del Caso de Prueba: Imprimir Constancia de verificación.			

Paso	Instrucción	Resultados Esperados	Observaciones / Comentarios
1	Ingresar al sistema Verificación de Documentos, seleccionar la opción de Imprimir.	Se mostrará una pantalla con una grilla de datos	
2	Hacer clic en el botón Imprimir.	Este proceso nos permitirá emitir la constancia de verificación del documento en donde se muestran los datos obtenidos del código en el proceso de decriptación incluyendo la fecha y hora en que fue verificado. En caso el proceso de verificación realizado al momento de escanear no haya sido satisfactorio no podrá imprimir esta constancia mostrando un mensaje de error .	

Caso de Prueba: 4	Opción : Borrar	Módulo : Verificación de Documentos	Estado del caso: APROBADO
Requisitos de Prueba: Ninguna			
Objetivo del Caso de Prueba: Se procede a blanquear la pantalla para iniciar un nuevo escaneo de documento.			

Paso	Instrucción	Resultados Esperados	Observaciones / Comentarios
1	Ingresar al sistema Verificación de Documentos, seleccionar la opción de Borrar.	Se mostrará una pantalla con una grilla de datos	
2	Hacer clic en el botón Borrar.	Este proceso nos permitirá limpiar la pantalla para iniciar una nueva verificación de documento.	

Caso de Prueba: 5	Opción : Ver Certificado	Módulo : Verificación de Documentos	Estado del caso: APROBADO
Requisitos de Prueba: Ninguna			
Objetivo del Caso de Prueba: Se visualiza certificado usado.			

Paso	Instrucción	Resultados Esperados	Observaciones / Comentarios
1	Ingresar al sistema Verificación de Documentos, seleccionar la opción de Ver Certificado.	Se mostrará una pantalla con una grilla de datos	
2	Hacer clic en el botón Ver Certificado.	Muestra las propiedades del certificado digital en uso.	

4.5 USO DE LAS METODOLOGIAS

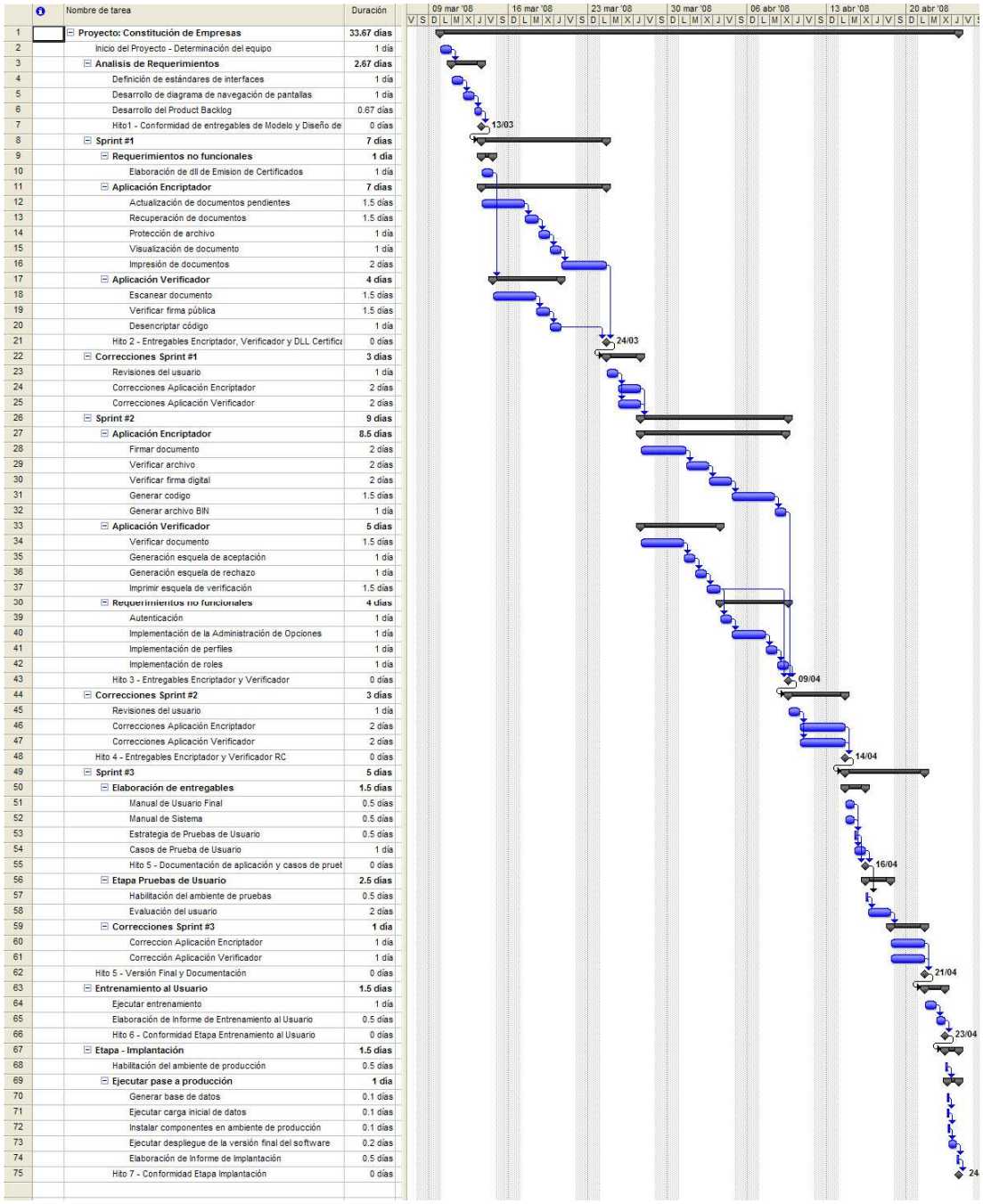
Para el desarrollo debía aprovecharse inteligentemente las metodologías dado el contexto del equipo y ambiente de trabajo. Teniendo eso en consideración se tomo lo mejor de SCRUM para gestión del proyecto y lo aplicable de XP desde el punto de vista de desarrollo de software.

4.5.1 APORTE DE SCRUM

Roles.- Desde el inicio del proyecto este fue reflejado en la definición de roles de parte del equipo. El clásico "Jefe de Proyecto", tomaría el rol del Scrum Master, al equipo de desarrollo se sumarían dos Analistas Programadores, conformando todos el Scrum Team y de la parte cliente (Product Owner) estaría el Colegio de Notarios de Lima, sumándose a la parte usuaria la Notaria Paíno.

Reuniones.- Establecidas específicamente para el equipo de desarrollo, estas se llevaron a cabo tal como lo sugiere la metodología de forma diaria. Buscando absolver las preguntas: "¿Qué se realizo el día anterior?", "¿Qué se hará el día de hoy?", "¿Necesitan alguna ayuda?". Se realizaron reuniones con el cliente como parte de las revisiones de los entregables.

Documentación.- La documentación de la parte de gestión la llevo el Scrum Master, que refleja 2 cosas, el Product Backlog de desarrollo y la parte complementaria como el entrenamiento y pruebas para lograr el producto final. Esto se puede ver en el Diagrama de Gantt que se muestra a continuación:



	Nombre de tarea	Duración
1	**Proyecto: Constitución de Empresas**	**33.67 días**
2	Inicio del Proyecto - Determinación del equipo	1 día
3	**Analisis de Requerimientos**	**2.67 días**
4	Definición de estándares de interfaces	1 día
5	Desarrollo de diagrama de navegación de pantallas	1 día
6	Desarrollo del Product Backlog	0.67 días
7	Hito1 - Conformidad de entregables de Modelo y Diseño de	0 días
8	**Sprint #1**	**7 días**
9	**Requerimientos no funcionales**	**1 día**
10	Elaboración de dll de Emision de Certificados	1 día
11	**Aplicación Encriptador**	**7 días**
12	Actualización de documentos pendientes	1.5 días
13	Recuperación de documentos	1.5 días
14	Protección de archivo	1 día
15	Visualización de documento	1 día
16	Impresión de documentos	2 días
17	**Aplicación Verificador**	**4 días**
18	Escanear documento	1.5 días
19	Verificar firma pública	1.5 días
20	Desencriptar código	1 día
21	Hito 2 - Entregables Encriptador, Verificador y DLL Certific	0 días
22	**Correcciones Sprint #1**	**3 días**
23	Revisiones del usuario	1 día
24	Correcciones Aplicación Encriptador	2 días
25	Correcciones Aplicación Verificador	2 días
26	**Sprint #2**	**9 días**
27	**Aplicación Encriptador**	**8.5 días**
28	Firmar documento	2 días
29	Verificar archivo	2 días
30	Verificar firma digital	2 días
31	Generar codigo	1.5 días
32	Generar archivo BIN	1 día
33	**Aplicación Verificador**	**5 días**
34	Verificar documento	1.5 días
35	Generación esquela de aceptación	1 día
36	Generación esquela de rechazo	1 día
37	Imprimir esquela de verificación	1.5 días
38	**Requerimientos no funcionales**	**4 días**
39	Autenticación	1 día
40	Implementación de la Administración de Opciones	1 día
41	Implementación de perfiles	1 día
42	Implementación de roles	1 día
43	Hito 3 - Entregables Encriptador y Verificador	0 días
44	**Correcciones Sprint #2**	**3 días**
45	Revisiones del usuario	1 día
46	Correcciones Aplicación Encriptador	2 días
47	Correcciones Aplicación Verificador	2 días
48	Hito 4 - Entregables Encriptador y Verificador RC	0 días
49	**Sprint #3**	**5 días**
50	**Elaboración de entregables**	**1.5 días**
51	Manual de Usuario Final	0.5 días
52	Manual de Sistema	0.5 días
53	Estrategia de Pruebas de Usuario	0.5 días
54	Casos de Prueba de Usuario	1 día
55	Hito 5 - Documentación de aplicación y casos de pruet	0 días
56	**Etapa Pruebas de Usuario**	**2.5 días**
57	Habilitación del ambiente de pruebas	0.5 días
58	Evaluación del usuario	2 días
59	**Correcciones Sprint #3**	**1 día**
60	Correccion Aplicación Encriptador	1 día
61	Corrección Aplicación Verificador	1 día
62	Hito 5 - Versión Final y Documentación	0 días
63	**Entrenamiento al Usuario**	**1.5 días**
64	Ejecutar entrenamiento	1 día
65	Elaboración de Informe de Entrenamiento al Usuario	0.5 días
66	Hito 6 - Conformidad Etapa Entrenamiento al Usuario	0 días
67	**Etapa - Implantación**	**1.5 días**
68	Habilitación del ambiente de producción	0.5 días
69	**Ejecutar pase a producción**	**1 día**
70	Generar base de datos	0.1 días
71	Ejecutar carga inicial de datos	0.1 días
72	Instalar componentes en ambiente de producción	0.1 días
73	Ejecutar despliegue de la versión final del software	0.2 días
74	Elaboración de Informe de Implantación	0.5 días
75	Hito 7 - Conformidad Etapa Implantación	0 días

Cronograma.- Scrum establece Sprints de 2-4 semanas. Aquí se hizo una variación de acuerdo a las funcionalidades que se realizaban, siendo estas de menor tiempo para poder hacer un seguimiento más preciso y adicionalmente se incorporo un tiempo de correcciones entre Sprints para minimizar el impacto que podría ocasionar en el Sprint siguiente y en perjuicio del proyecto.

4.5.2 APORTE DE XP

La Extreme Programming contribuyo desde la perspectiva de desarrollo de la aplicación, mas no se siguieron todas las prácticas que sugiere la metodología porque el equipo está acostumbrado a otra forma de trabajo y los cambios debían ser graduales.

Entre las prácticas de XP que se tomaron en consideración para el proyecto se encuentran:

Estándares de codificación.- Se utilizó el estándar de codificación existente en la empresa.

Diseño Simple.- Se codifico lo estrictamente necesario en base a las funcionalidades o casos de uso establecido por Sprint.

Pruebas continuas.- Durante el desarrollo se realizaron pruebas de parte del mismo equipo y estas se complementaban con las revisiones de parte del cliente.

Versiones pequeñas.- Esto permitía mostrar al cliente avances de las funcionalidades desarrolladas completas.

Algunas otras no se podían aplicar porque el equipo tenía un acceso limitado al cliente y se debía desplazarse al local de los Product Owner o usuarios. Otra práctica mencionada en la XP es la programación en pareja, en este caso las aplicaciones de encriptación y verificación estaban asignadas a los dos analistas programadores y uno de ellos era responsable de la parte de encriptación y el otro de la verificación.

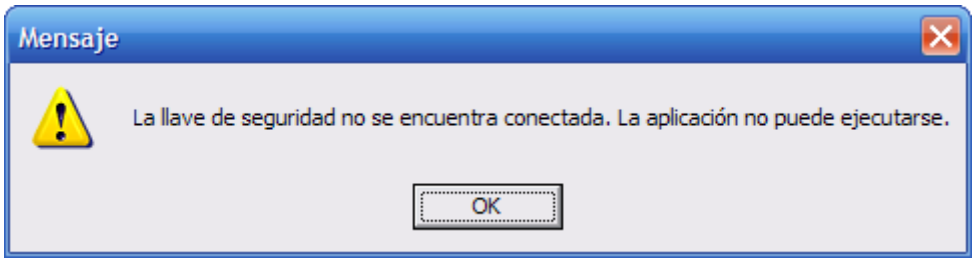
4.6 DESCRIPCION DE SOFTWARE PROPUESTO

4.6.1 APLICACIÓN ENCRIPTADOR

Funcionalidad

Esta aplicación tiene la siguiente funcionalidad:

La primera validación que el sistema realiza es la presencia de la llave de seguridad ETOKEN la cual deberá estar conecta a un puerto USB en el ordenador donde se intenta ejecutar la aplicación. Si no se cuenta con la llave de seguridad ETOKEN, muestra el siguiente mensaje:

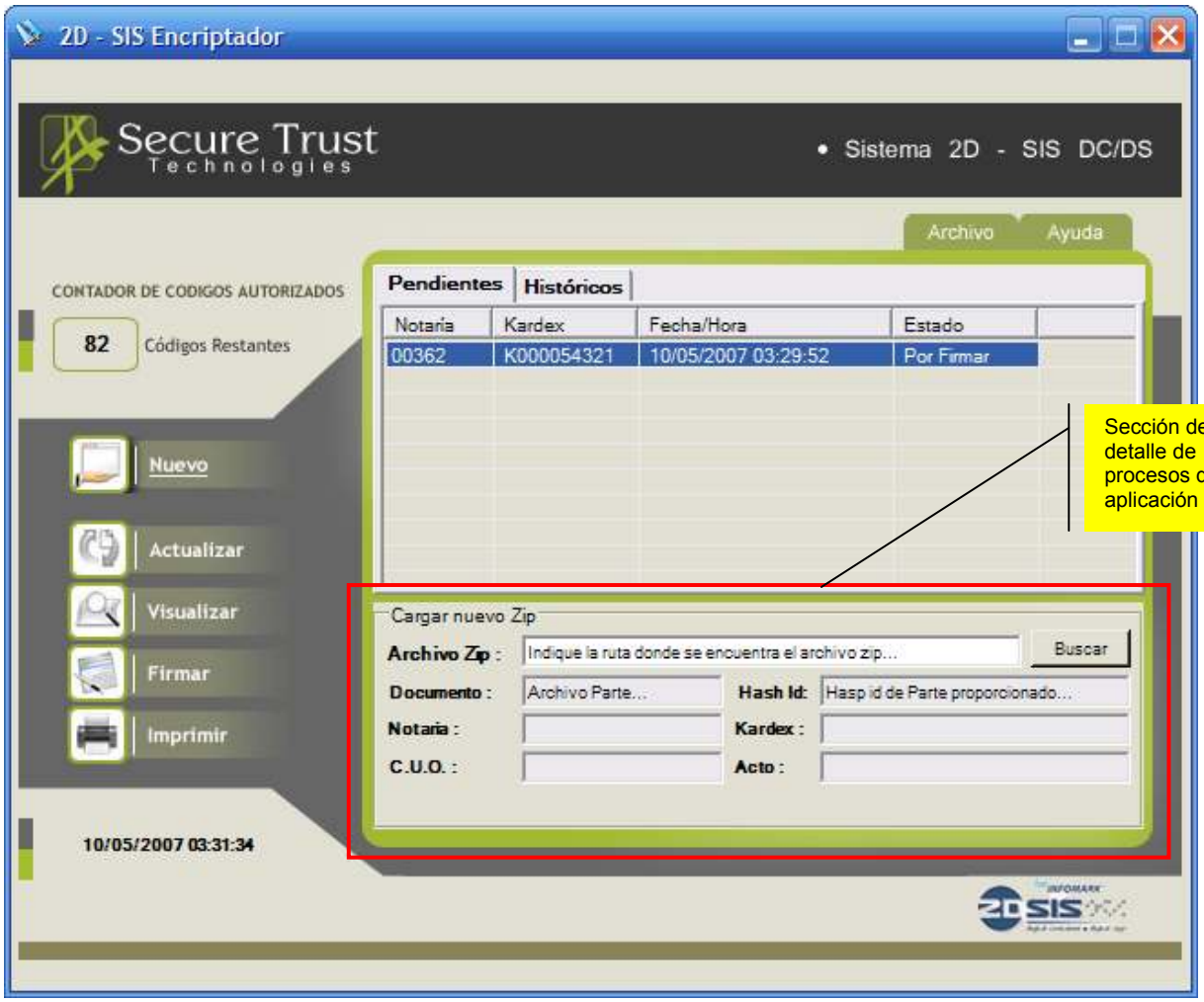


Esta llave, además de estar programa para proteger el acceso a la aplicación Encriptador, lleva el contador de códigos autorizados con el que controla en número impresiones permitidas. Este contador será visualizado en la máscara del sistema en la sección “Contador de Códigos Autorizados”.

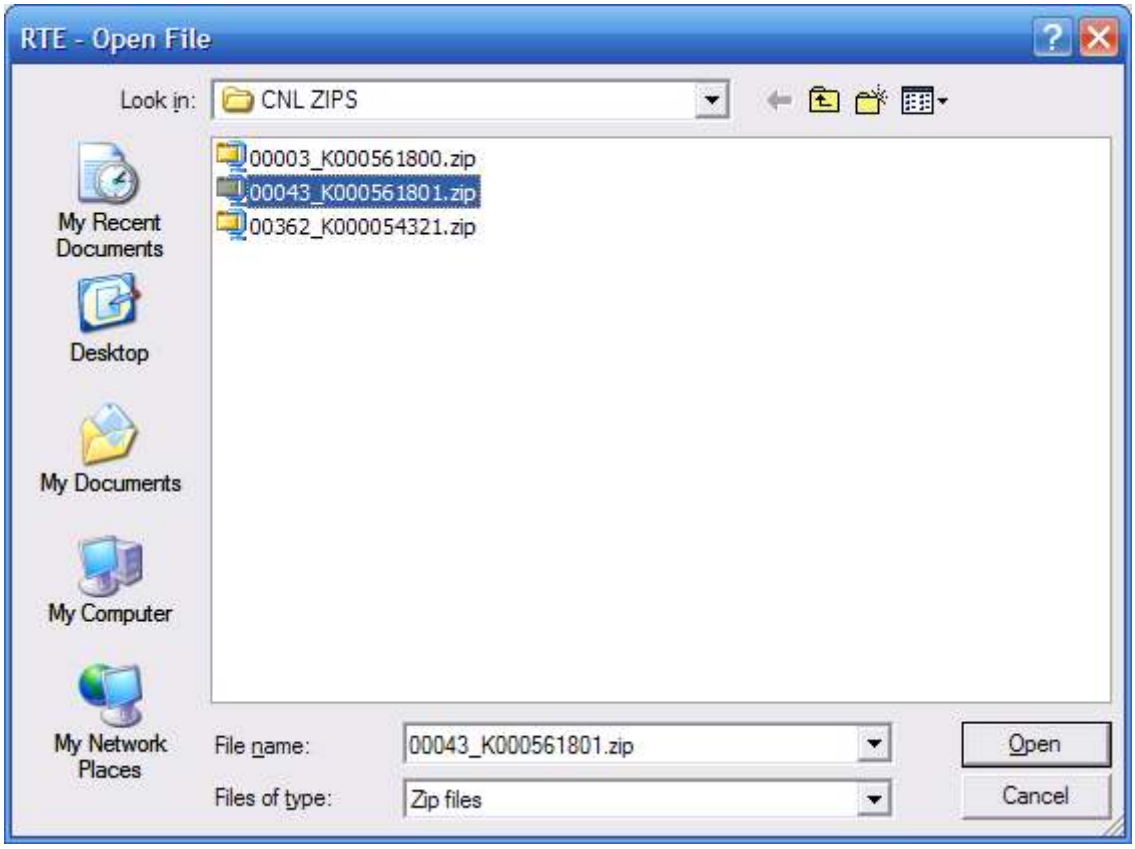
PROCESO NUEVO

La funcionalidad de este proceso es permitir al usuario cargar un nuevo documento dentro del repositorio seguro del Sistema de Protección de Archivos.

Al hacer clic en el botón Nuevo se mostrará la opción “Cargar Nuevo Zip” en la sección de detalle de procesos de la aplicación.



Haciendo clic en el botón “Buscar”, seleccionamos la ruta desde donde se van cargar los archivos de formato **.zip**.



El archivo zip contendrá 2 archivos, un documento de extensión RTF, que es el documento sensible que se quiere proteger y uno de extensión TXT que contiene una sumilla del documento RTF en donde se almacenan los datos que identifican al documento.

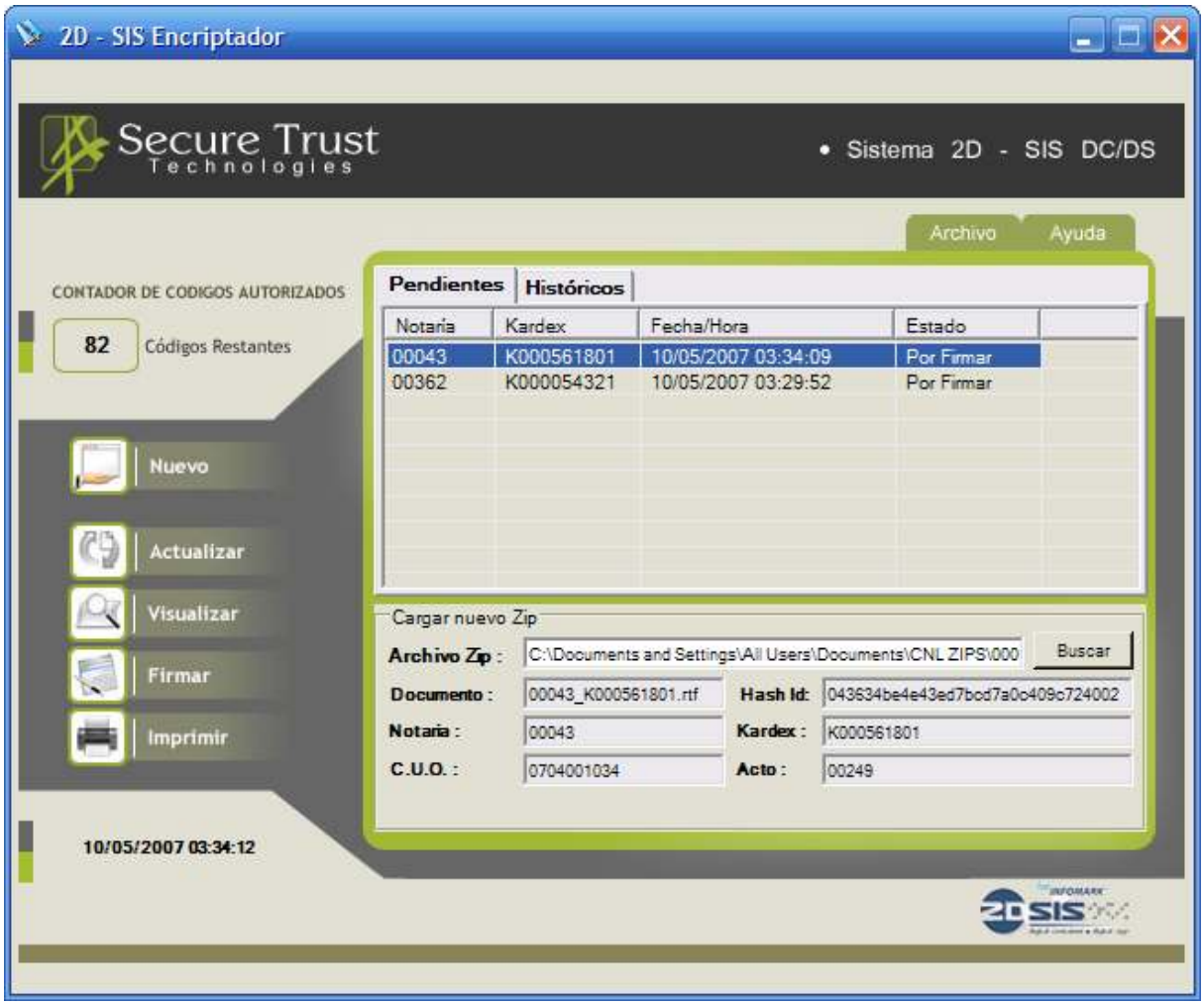
Confirmado el archivo que será cargado la aplicación internamente realiza el proceso de descompresión de archivo zip y procede a proteger los archivos, cifrándolos y haciendo uso de la firma digital propietaria de la aplicación EntersysSender.

Así mismo se obtiene el hash del documento RTF (utilizando el algoritmo de MD5) y éste se verifica contra el hash que se obtiene de la sumilla; se procede hacer la comparación de hashes y si los códigos coinciden la aplicación mostrará el mensaje de confirmación de carga realizada correctamente.

Y se procede a encriptar el contenido de cada documento y colocarlos en el repositorio de la aplicación en estado Por Firmar.

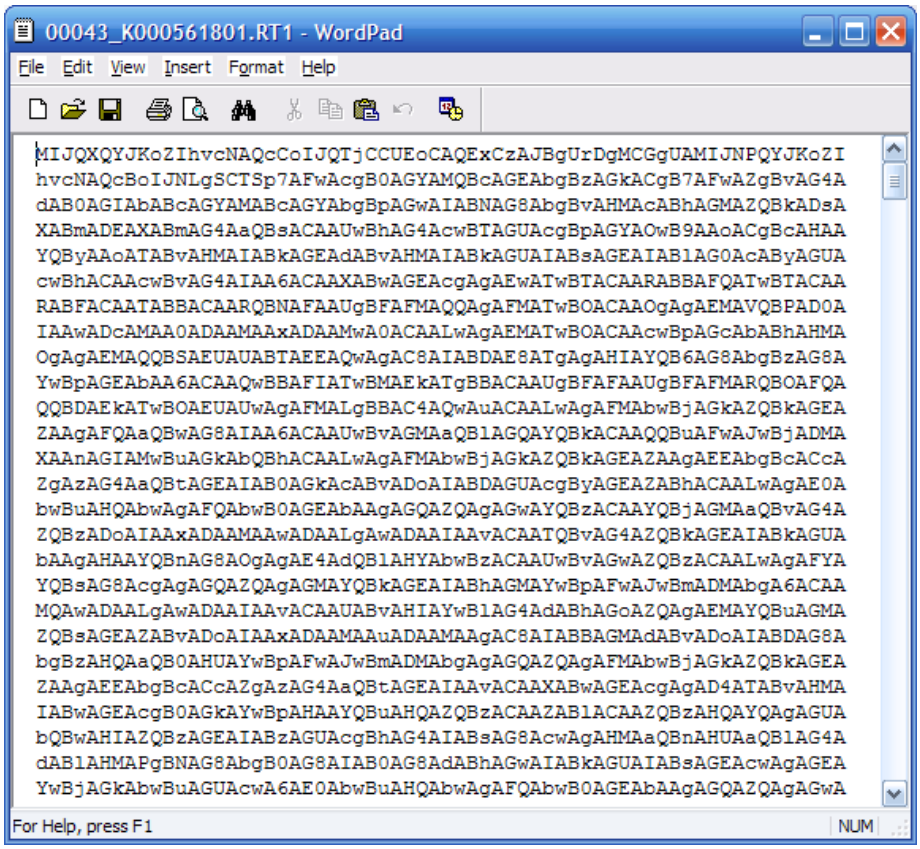
Nota.-

Para este procedimiento se hace uso del método de cifrado simétrico, lo que quiere decir que se utilizará sólo un juego de firmas, una privada (firma propietaria EntersysSender) para encriptar el documento y otra pública que será usada para verificarlo posteriormente.



En caso de que NO se dé el matching entre los hashes el proceso de carga se invalida.

Si se abre el archivo encriptado se visualizará de la siguiente manera:



Esto nos indica que el contenido del archivo original no puede ser entendido por cualquier usuario una vez que el documento es cargado en la aplicación.

Y en caso que el archivo sea modificado en su contenido el algoritmo de Verificación de Firma Privada no lo reconocerá cuando intente ser visualizado, firmado o impreso en la aplicación, lo cual obviamente invalida dicho documento.

PROCESO ACTUALIZAR

La funcionalidad que se cumple aquí es la de Refrescar la pantalla, recorriendo la carpeta o repositorio de la aplicación para cargar en la grilla los nuevos archivos pendientes en estado **Por Firmar** o **Por Imprimir**. En la sección de detalle de procesos de la aplicación podemos observar los datos del documento seleccionado tales como:

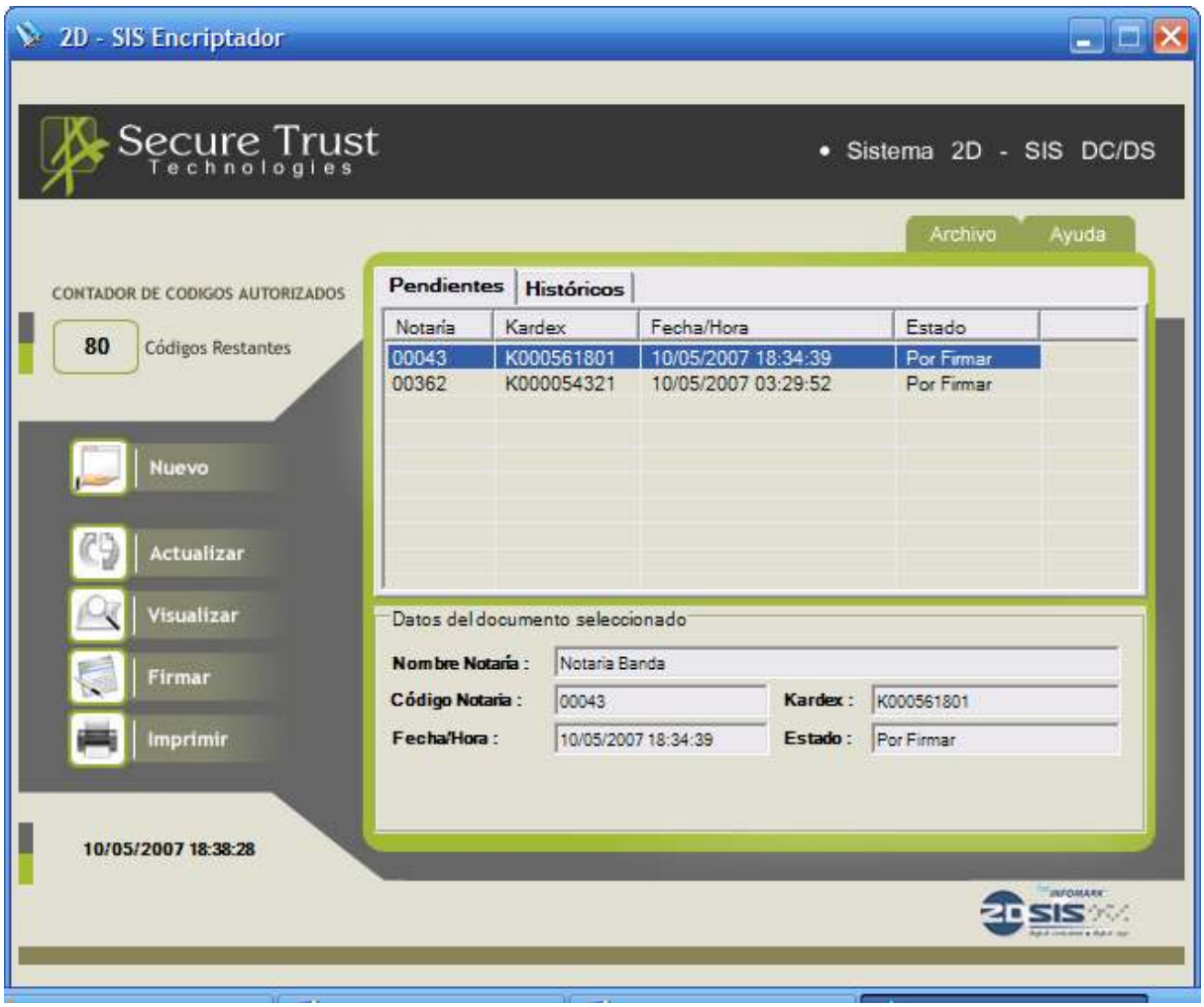
Nombre de Notaría

Código de Notaria

Fecha / Hora de creación

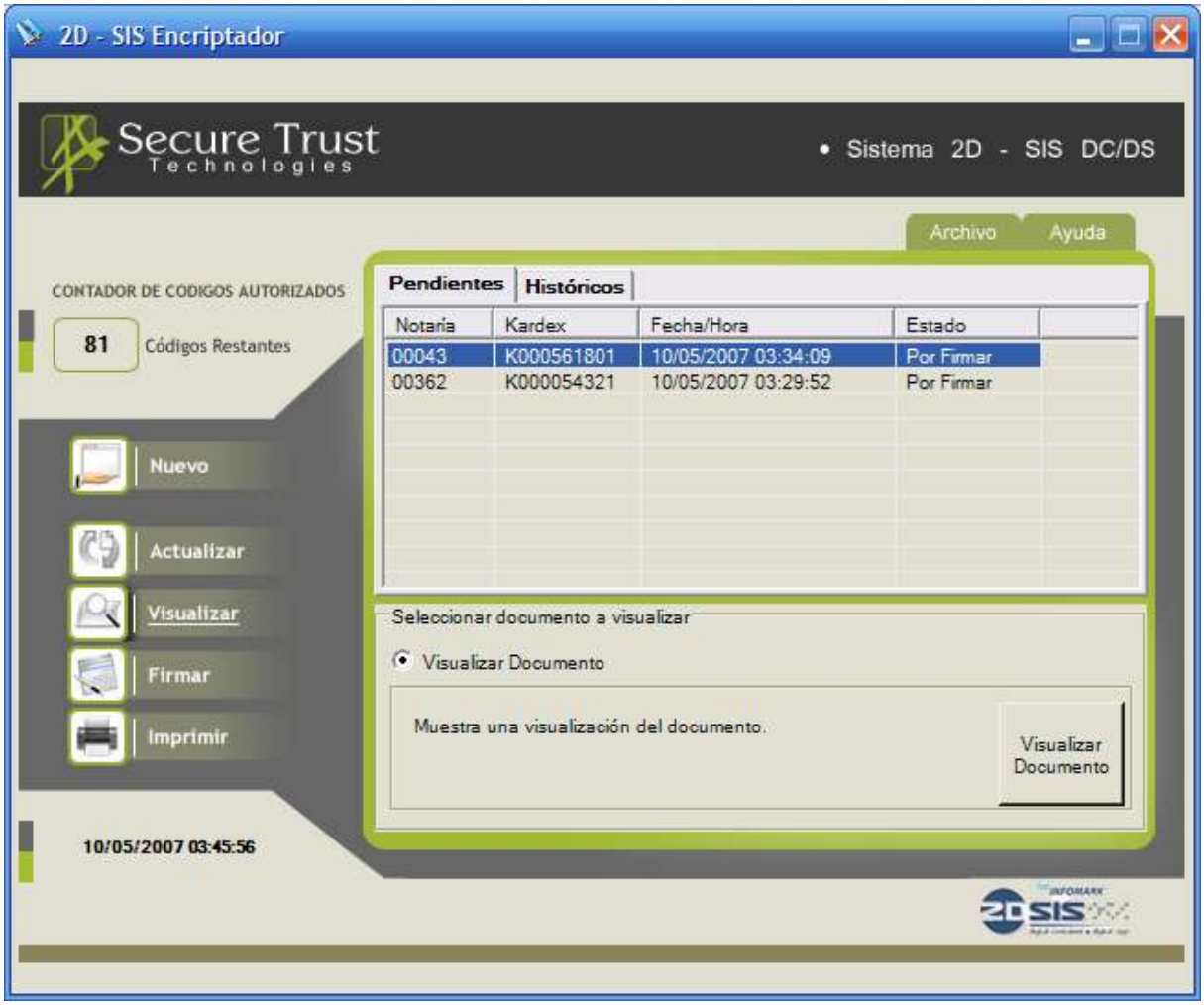
Kardex

Estado del documento.

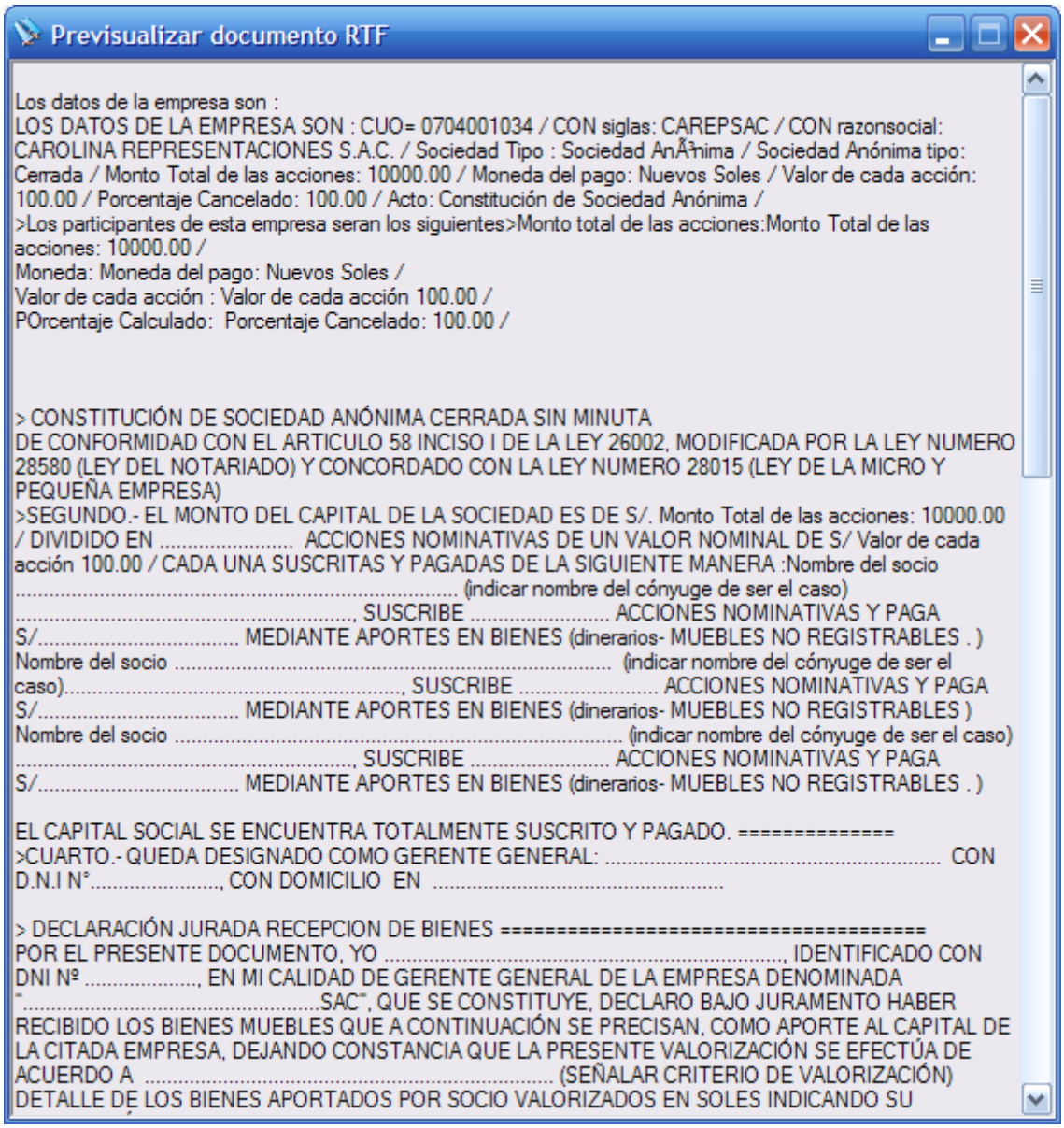


PROCESO VISUALIZAR

Aquí podemos visualizar los documentos que se encuentren en los estados Por Firmar, Por Imprimir mostrados en la bandeja de Pendientes, o estado Cerrado que se encuentran en la bandeja de Históricos.



En la sección de detalle de procesos de la aplicación contamos con el botón de "Visualizar Documento" que nos permite abrir una ventana en la que se pre-visualiza el contenido del documento.

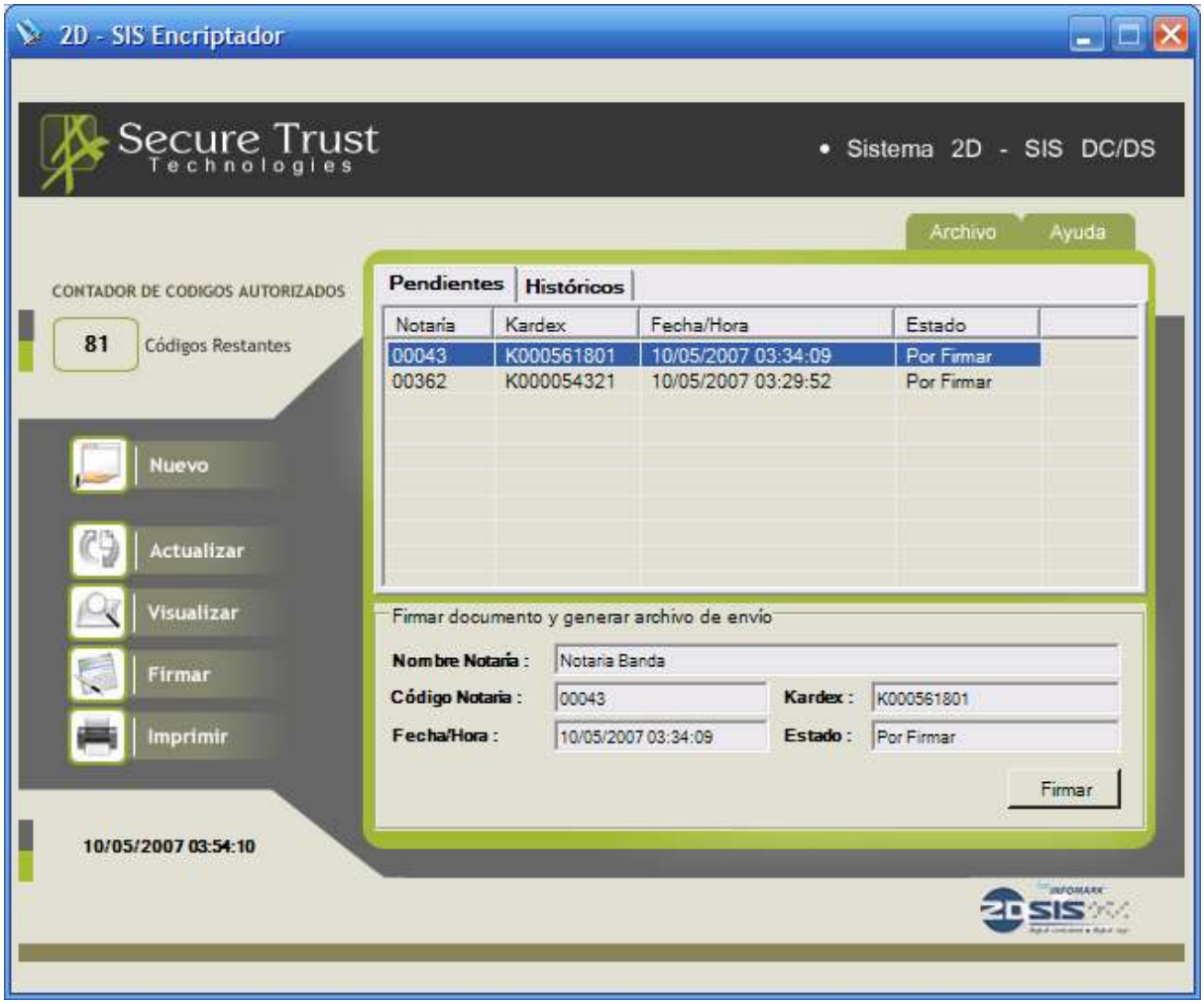


Nota.-

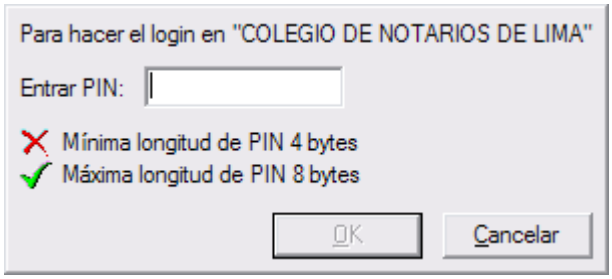
Para poder visualizar el documento se realiza un proceso de *Verificación de Firma* (haciendo uso de la firma propietaria EntersysSender) ya que el archivo se encuentra encriptado desde que fue cargado en el repositorio. El documento sólo se visualizará en caso que la verificación de la firma propietaria sea satisfactoria lo cual nos indica que el archivo no ha sido alterado en su contenido.

PROCESO FIRMAR

En la sección de detalle de procesos de la aplicación, se muestra la opción Firmar documento y generar archivo de envío.

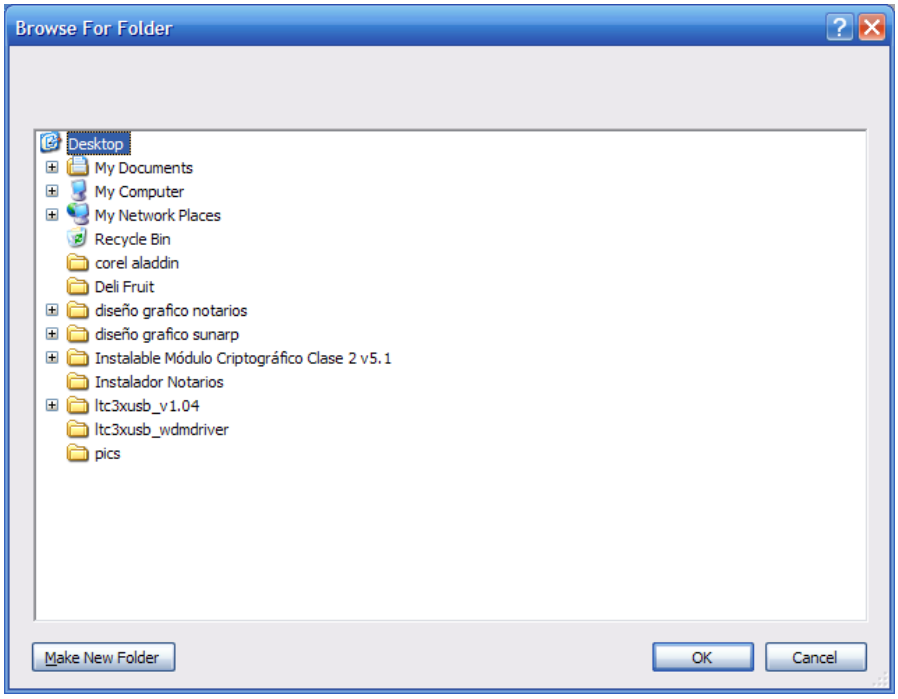


Hacemos clic en el botón “Firmar” e inmediatamente se cargará una ventana solicitando ingresar el PIN o código secreto de la Autoridad Firmante.



Para esto se debe contar con el Smart Card y la tarjeta chip de memoria protegida que contiene la Firma Digital de la Autoridad Firmante.

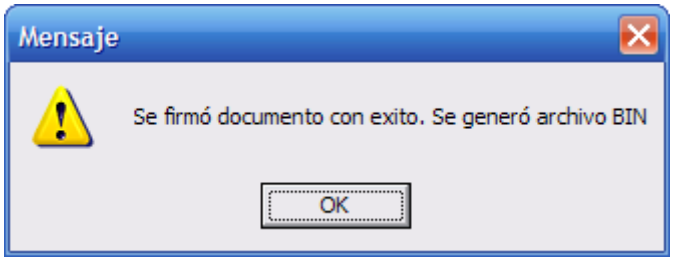
En seguida de ingresado el PIN, se carga la ventana en la que se seleccionará la ruta donde se generará el archivo de tipo BIN que es el “Archivo ya Firmado”.



Hacemos clic en botón “OK” y con esto estamos encriptando el documento con la Firma Digital Privada del Notario obtenida del dispositivo externo SMART CARD.

El archivo generado en este proceso (extensión BIN) es el que se enviará electrónicamente al Organismo Receptor del documento.

Una vez firmado digitalmente el documento se muestra un mensaje de confirmación, en el que nos indica que se generó el archivo correctamente.



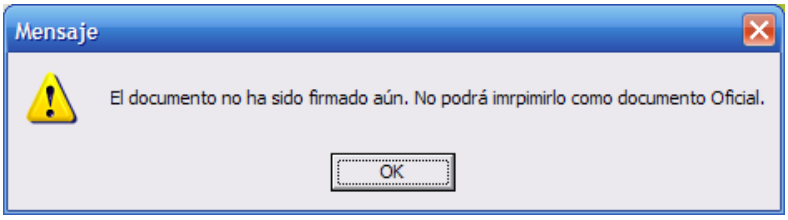
Notas.-

La aplicación no permite firmar dos veces un mismo documento así que en caso de seleccionar un documento que haya sido firmado previamente mostrará el mensaje de error correspondiente.

Para poder visualizar el documento se realiza un proceso de *Verificación de Firma* (haciendo uso de la firma propietaria EntersysSender) ya que el archivo se encuentra encriptado desde que fue cargado en el repositorio. El documento sólo se visualizará en caso que la verificación de la firma propietaria sea satisfactoria lo cual nos indica que el archivo no ha sido alterado en su contenido.

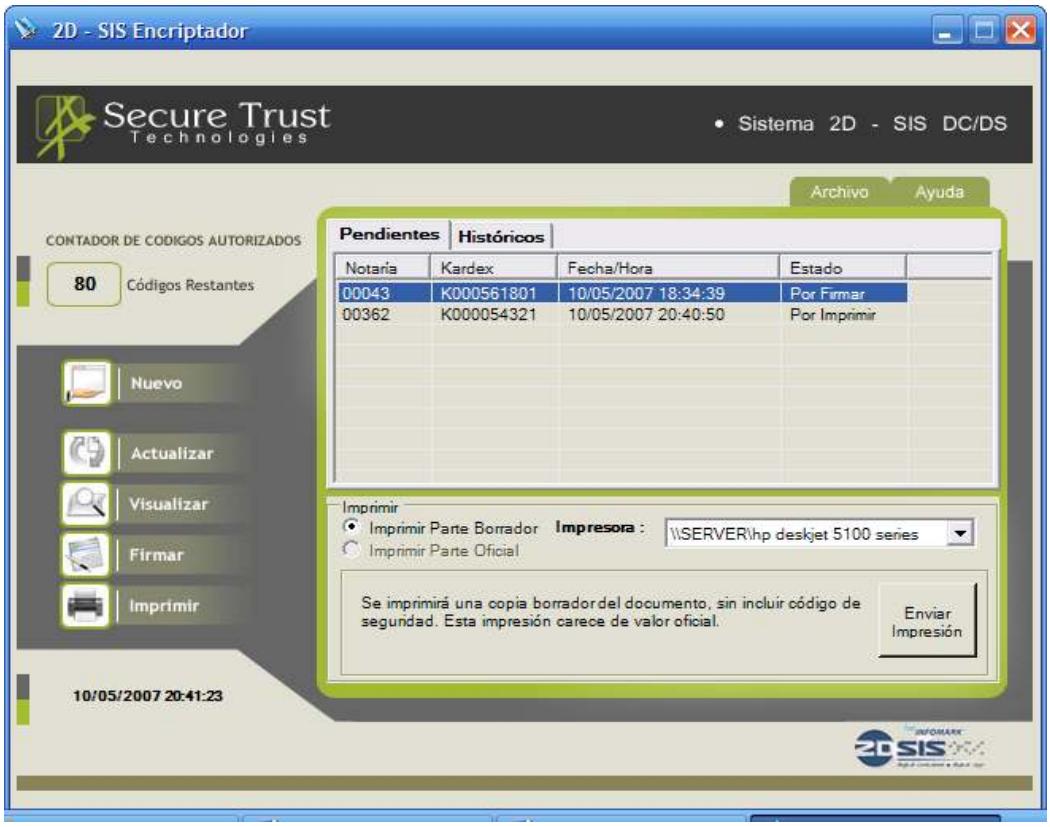
PROCESO IMPRIMIR

En la sección de detalle de procesos de la aplicación, se muestra la opción Imprimir.
En este proceso solo permite imprimir los documentos que ya han sido firmados así que en caso de seleccionar un registro que no cumpla con dicha validación se mostrará el mensaje de error correspondiente.

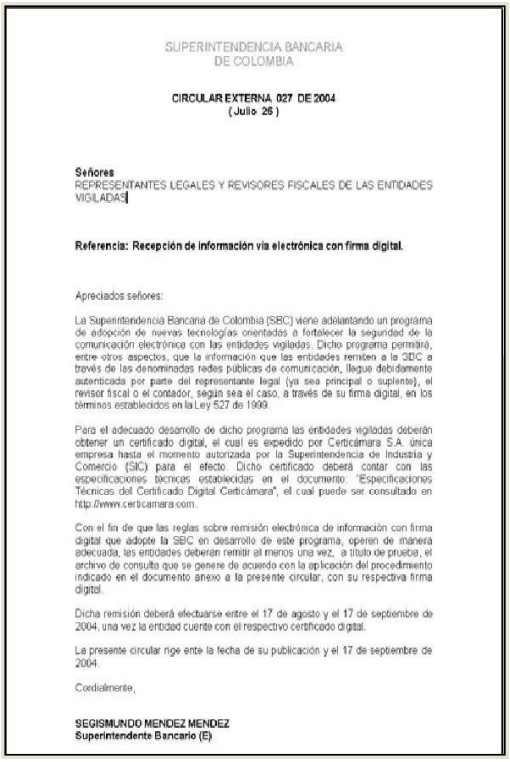


Funcionalmente este proceso tiene dos opciones de impresión que describimos a continuación:

Imprimir Parte Borrador: permite imprimir el documento RTF original sin el código esteganográfico.



Al hacer clic en el botón Enviar Impresión, físicamente el documento se imprime tal cual:



SUPERINTENDENCIA BANCARIA
DE COLOMBIA

CIRCULAR EXTERNA 027 DE 2004
(Julio 26)

Señores
REPRESENTANTES LEGALES Y REVISORES FISCALES DE LAS ENTIDADES VIGILADAS

Referencia: Recepción de información vía electrónica con firma digital.

Apreciados señores:

La Superintendencia Bancaria de Colombia (SBC) viene adelantando un programa de adopción de nuevas tecnologías orientadas a fortalecer la seguridad de la comunicación electrónica con las entidades vigiladas. Dicho programa permitirá, entre otros aspectos, que la información que las entidades remiten a la SBC a través de las denominadas redes públicas de comunicación, llegue debidamente autenticada por parte del representante legal (ya sea principal o suplente), el revisor fiscal o el contador, según sea el caso, a través de su firma digital, en los términos establecidos en la Ley 527 de 1999.

Para el adecuado desarrollo de dicho programa las entidades vigiladas deberán obtener un certificado digital, el cual es expedido por Certicámara S.A. única empresa hasta el momento autorizada por la Superintendencia de Industria y Comercio (SIC) para el efecto. Dicho certificado deberá contar con las especificaciones técnicas establecidas en el documento "Especificaciones Técnicas del Certificado Digital Certicámara", el cual puede ser consultado en http://www.certicamara.com.

Con el fin de que las reglas sobre remisión electrónica de información con firma digital que adopte la SBC en desarrollo de este programa, operen de manera adecuada, las entidades deberán remitir al menos una vez, a título de prueba, el archivo de consulta que se genere de acuerdo con la aplicación del procedimiento indicado en el documento anexo a la presente circular, con su respectiva firma digital.

Dicha remisión deberá efectuarse entre el 17 de agosto y el 17 de septiembre de 2004, una vez la entidad cuente con el respectivo certificado digital.

La presente circular rige ente la fecha de su publicación y el 17 de septiembre de 2004.

Cordialmente,

SEGISMUNDO MENDEZ MENDEZ
Superintendente Bancario (E)

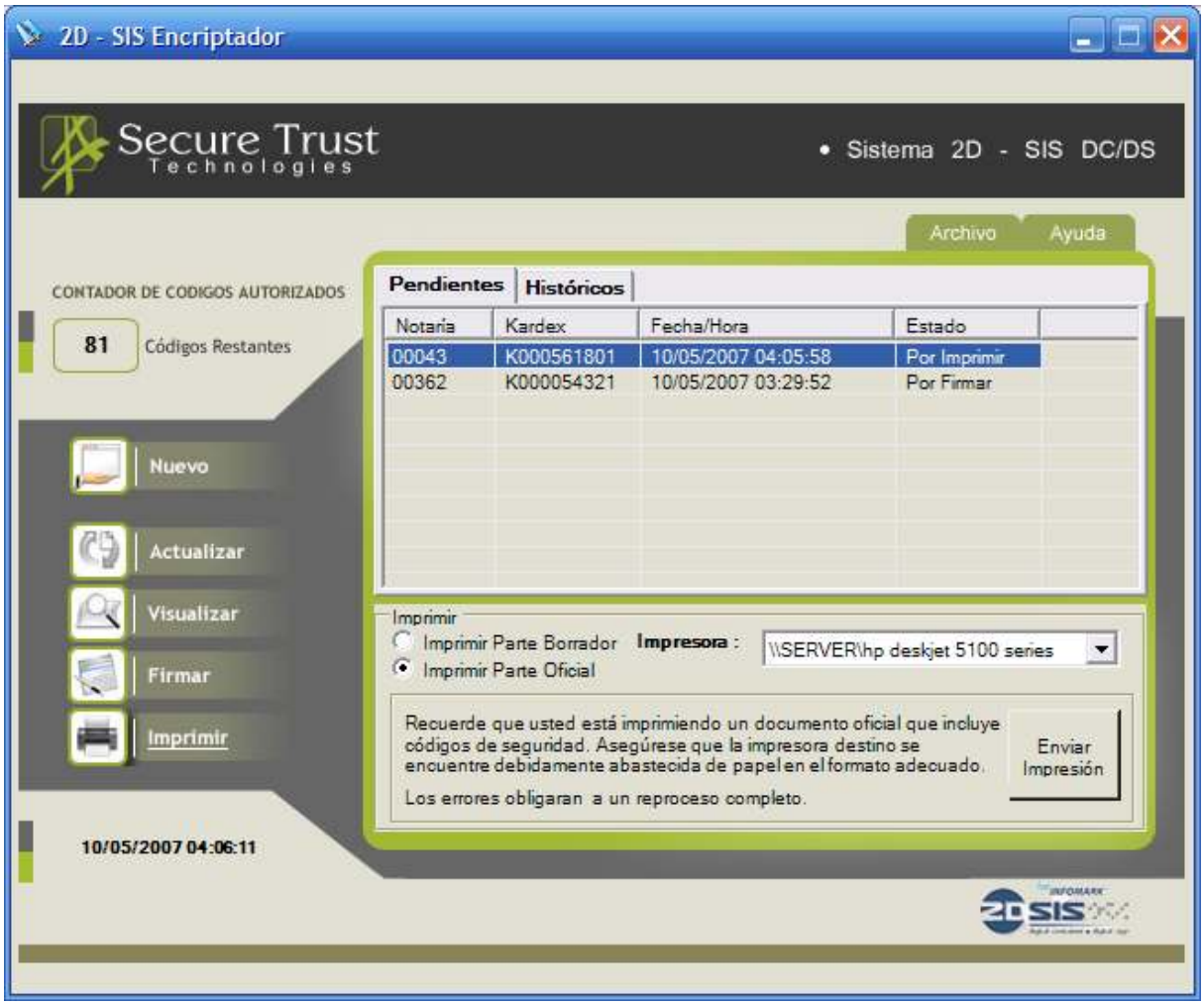
DOCUMENTO ORIGINAL

Impresión de documento original

Imprimir Parte Oficial: permite imprimir el documento RTF original con el Contenedor Digital Análogo (Código Esteganográfico), el cual solo será generado sólo si han sido instalados los certificados digitales correspondientes a las firmas propietarias de la aplicación EntersysSender y EntersysReceiver. Dicho código encriptará e incluirá en él los datos obtenidos de la sumilla (archivo TXT) en donde incrusta el hash del documento digital que será usado para la validación del documento en el organismo receptor.

Nota.-

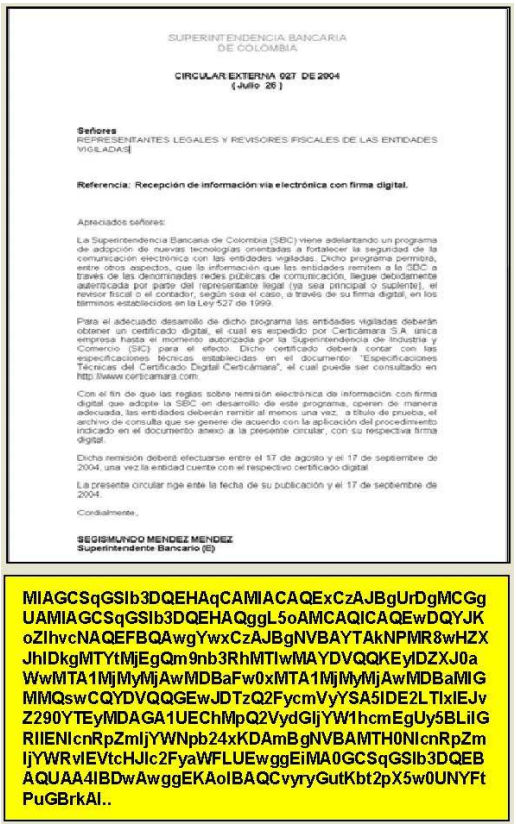
El contenedor digital se genera haciendo uso del método de cifrado asimétrico el cual requiere un par de juegos de firmas digitales. Esto significa que se necesitará una clave privada y una pública para encriptarlo y su contraparte al momento de verificarlo.



Al hacer clic en el botón Enviar Impresión, la aplicación verificará la existencia de Códigos Autorizados, los cuales serán leídos de la llave de seguridad ETOKEN.

En caso de no contar con códigos restantes no se permitirá la impresión oficial del documento.

Físicamente el documento se imprime con código esteganográfico:



SUPERINTENDENCIA BANCARIA
DE COLOMBIA

CIRCULAR EXTERNA 027 DE 2004
(Julio 26)

Señores
REPRESENTANTES LEGALES Y REVISORES FISCALES DE LAS ENTIDADES VIGILADAS

Referencia: Recepción de información vía electrónica con firma digital.

Apreciados señores:

La Superintendencia Bancaria de Colombia (SBC) viene adelantando un programa de adopción de nuevas tecnologías orientadas a fortalecer la seguridad de la comunicación electrónica con las entidades vigiladas. Dicho programa permitirá, entre otros aspectos, que la información que las entidades remiten a la SBC a través de las denominadas redes públicas de comunicación, llegue debidamente autenticada por parte del representante legal (ya sea principal o suplente), el revisor fiscal o el contador, según sea el caso, a través de su firma digital, en los términos establecidos en la Ley 527 de 1999.

Para el adecuado desarrollo de dicho programa las entidades vigiladas deberán obtener un certificado digital, el cual es expedido por Certicámara S.A. única empresa hasta el momento autorizada por la Superintendencia de Industria y Comercio (SIC) para el efecto. Dicho certificado deberá contar con las especificaciones técnicas establecidas en el documento "Especificaciones Técnicas del Certificado Digital Certicámara", el cual puede ser consultado en http://www.certicamara.com.

Con el fin de que las reglas sobre remisión electrónica de información con firma digital que adopte la SBC en desarrollo de este programa, operen de manera adecuada, las entidades deberán remitir al menos una vez, a título de prueba, el archivo de consulta que se genere de acuerdo con la aplicación del procedimiento indicado en el documento anexo a la presente circular, con su respectiva firma digital.

Dicha remisión deberá efectuarse entre el 17 de agosto y el 17 de septiembre de 2004, una vez la entidad cuente con el respectivo certificado digital

La presente circular rige ente la fecha de su publicación y el 17 de septiembre de 2004.

Cordialmente,

SEGISMUNDO MENDEZ MENDEZ
Superintendente Bancario (E)

"HASH" o huella que se obtiene a partir del documento.

Impresión de documento firmado digitalmente

Un vez impreso el documento oficial el estado del archivo pasa a "Cerrado" y se envía a la carpeta Históricos.

Notas.-

La aplicación no permite imprimir oficialmente dos veces un mismo documento así que en caso de seleccionar un documento que haya sido impreso en esta opción previamente mostrará el mensaje de error correspondiente.

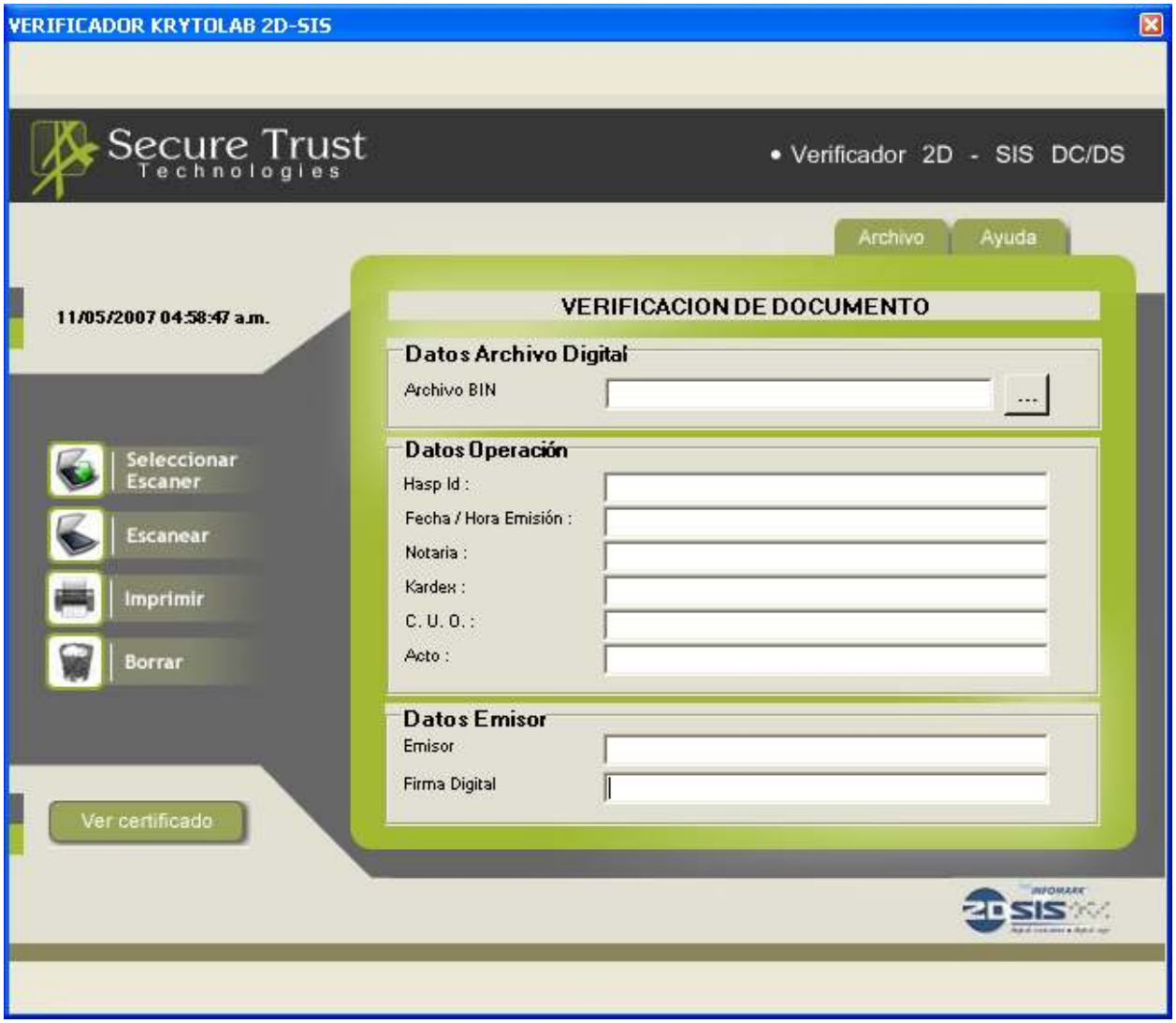
Para poder imprimir el documento original, tanto en borrador como oficial, se debe realizar también el proceso de *Verificación de Firma Propietaria* para desencriptar el archivo. El documento sólo se imprimirá en caso que la verificación de la firma propietaria sea satisfactoria lo cual nos indica que el archivo no ha sido alterado en su contenido.

4.6.2 APLICACIÓN VERIFICADOR

Funcionalidad

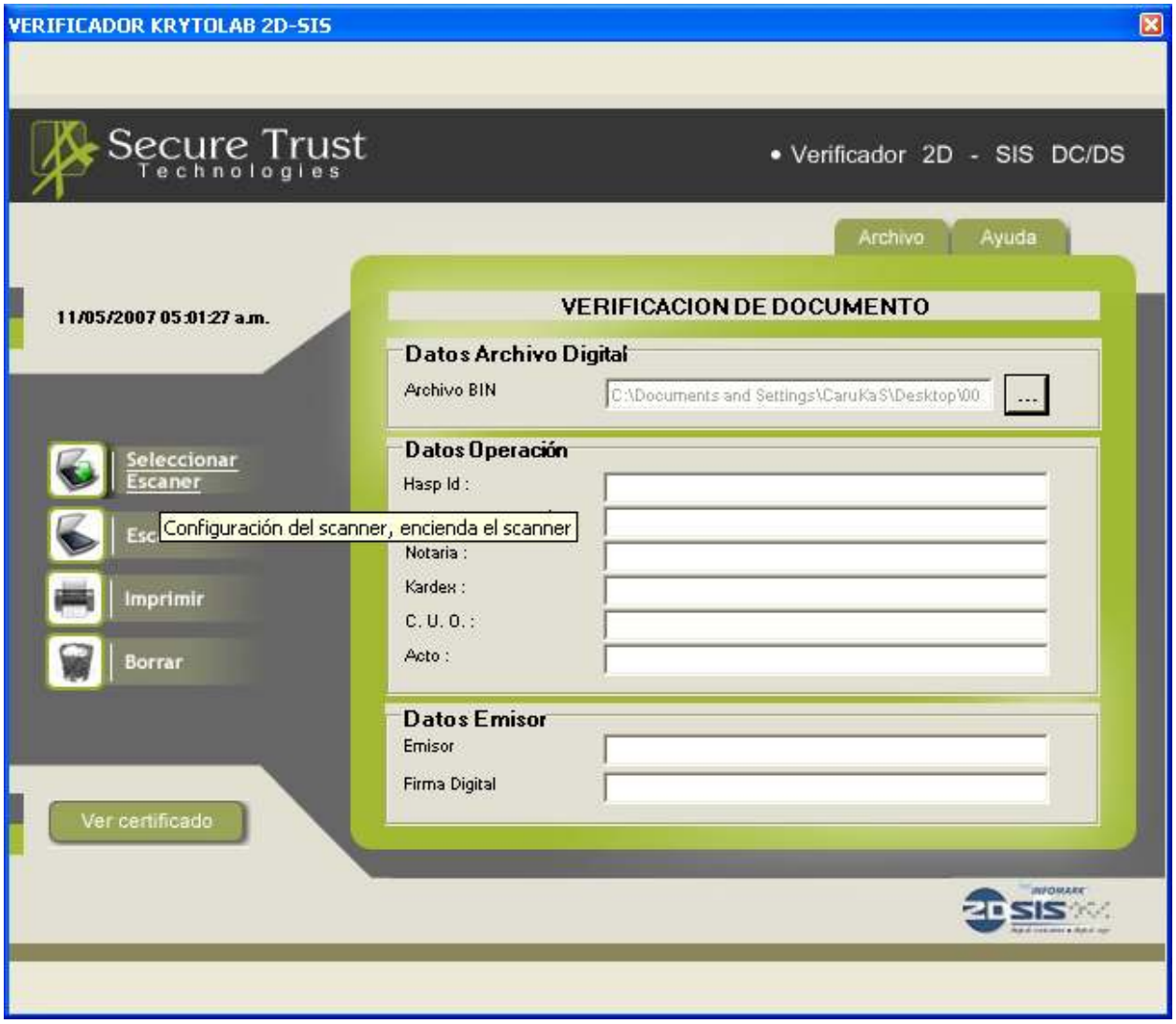
Esta aplicación tiene la siguiente funcionalidad:

Cuenta con una pantalla principal en donde se pueden realizar las operaciones de Escanear el documento impreso, Imprimir constancia de verificación del documento, Seleccionar Escaner y Limpiar pantalla.

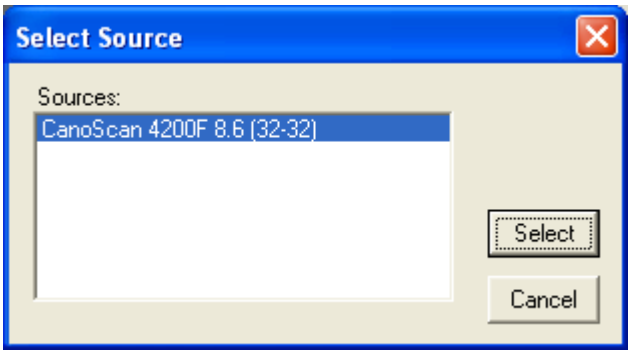


PROCESO SELECCIONAR ESCANER

Este proceso nos permitirá seleccionar el dispositivo externo mediante el cual se realizará el proceso de escaneo del documento.



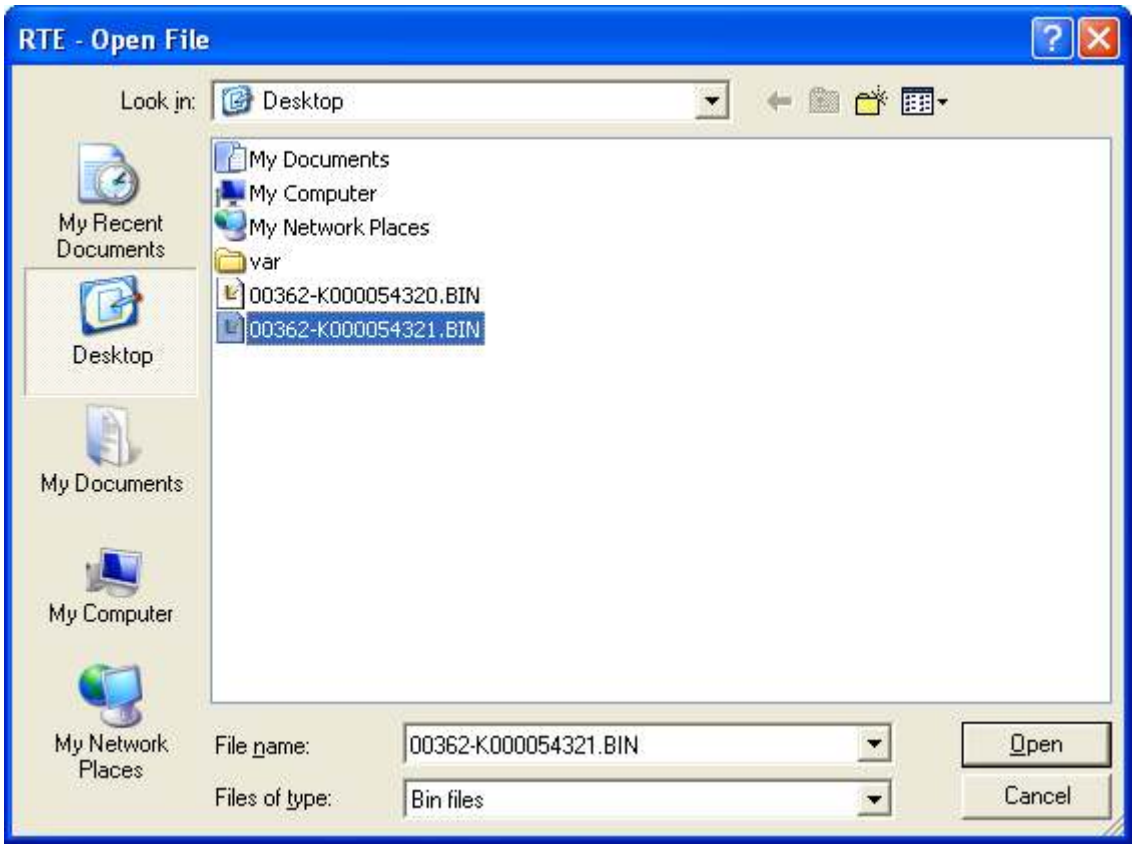
Al hacer clic sobre el botón “Seleccionar Escaner” nos mostrará la ventana de selección del dispositivo deseado:



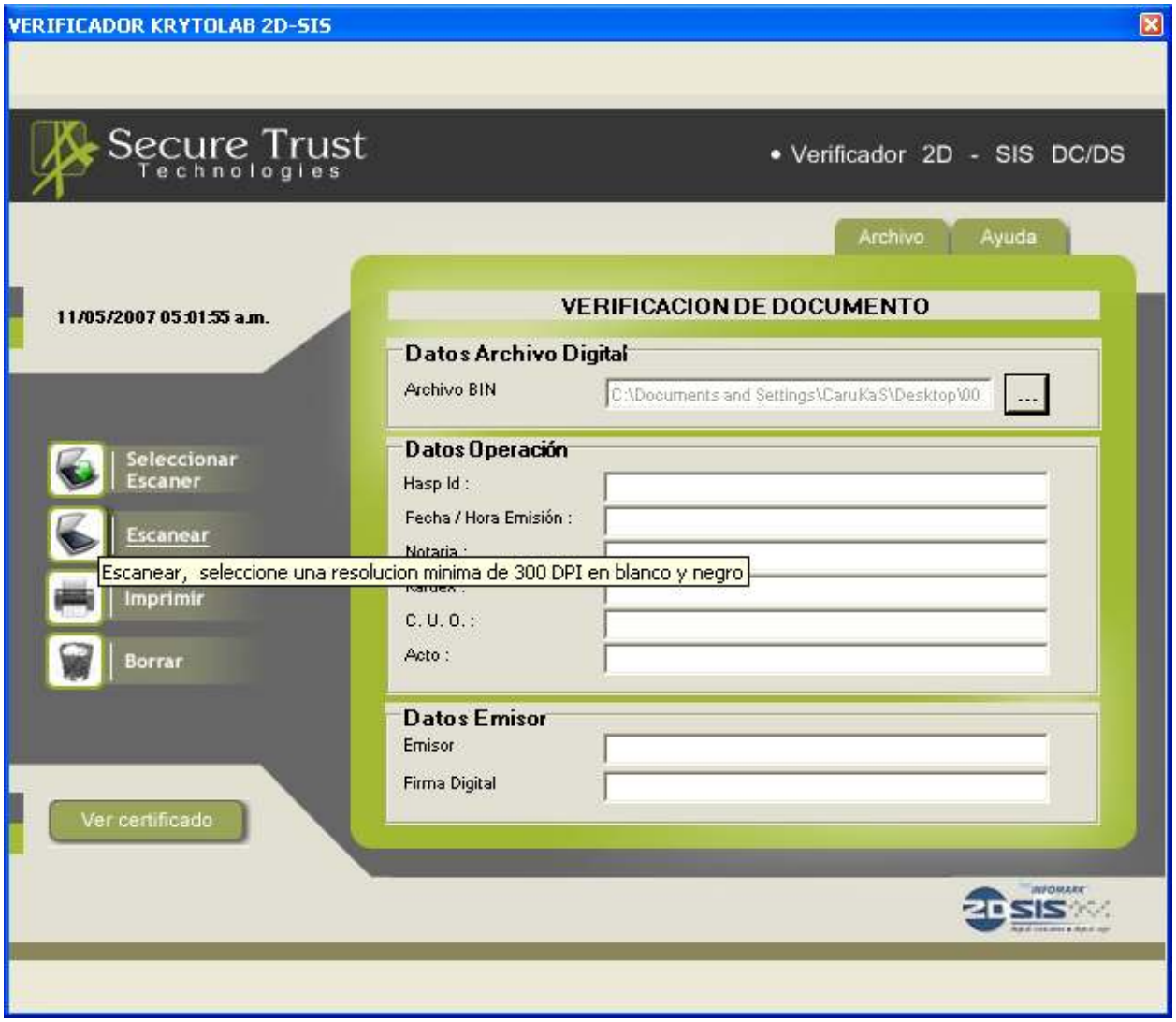
PROCESO ESCANEAR

Este proceso nos permitirá la digitalización de los datos contenidos en el código esteganográfico mediante los cuales de verificará la validez del documento digital a través de la comparación de hashes.

El primer paso para este proceso es seleccionar el archivo BIN que será objeto de verificación, para esto hacemos clic en el botón Browse  e inmediatamente aparecerá un cuadro de dialogo en donde podemos indicar la ruta del archivo.

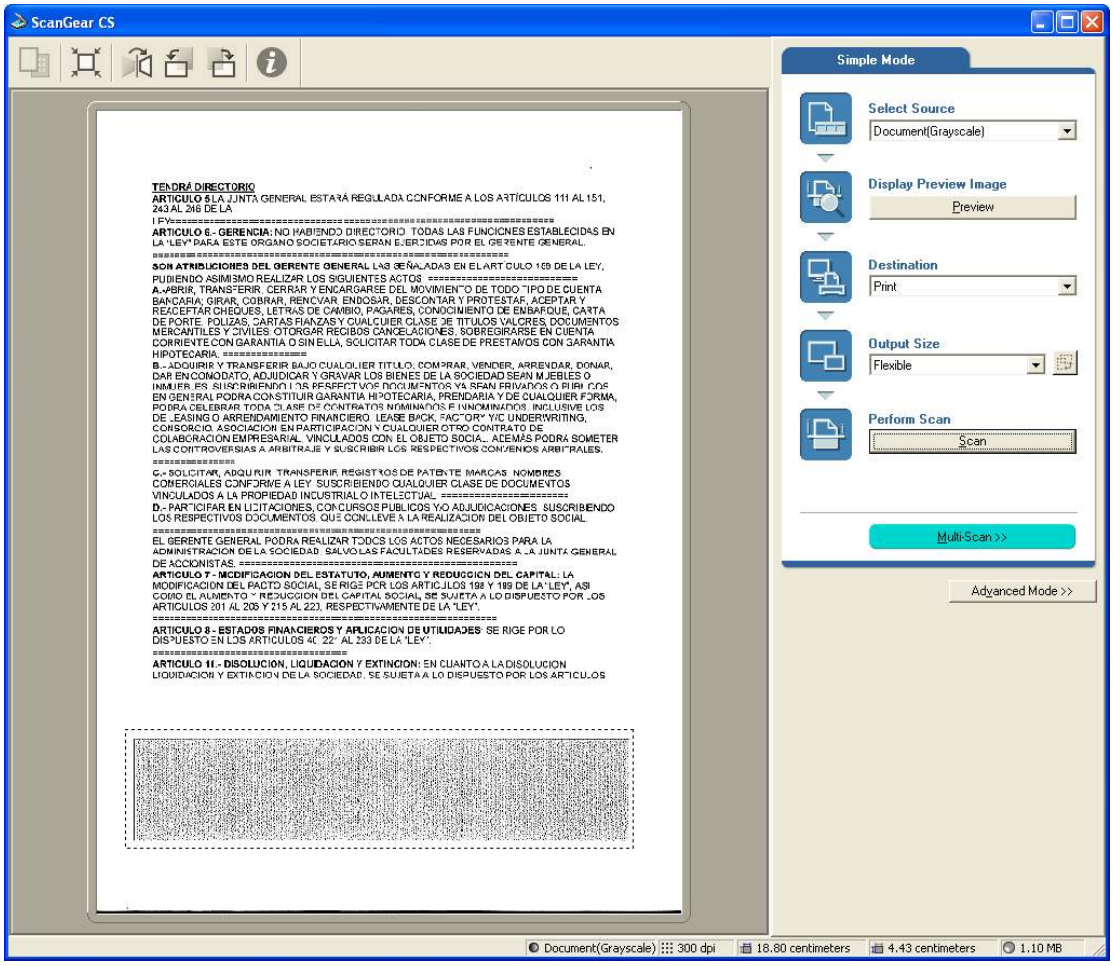


Una vez cargado el archivo procedemos a colocar en el escáner una de las hojas del documento impreso y hacemos clic en el botón “Escanear”



En caso de no haber cargado previamente el archivo BIN se mostrará el siguiente mensaje de error:

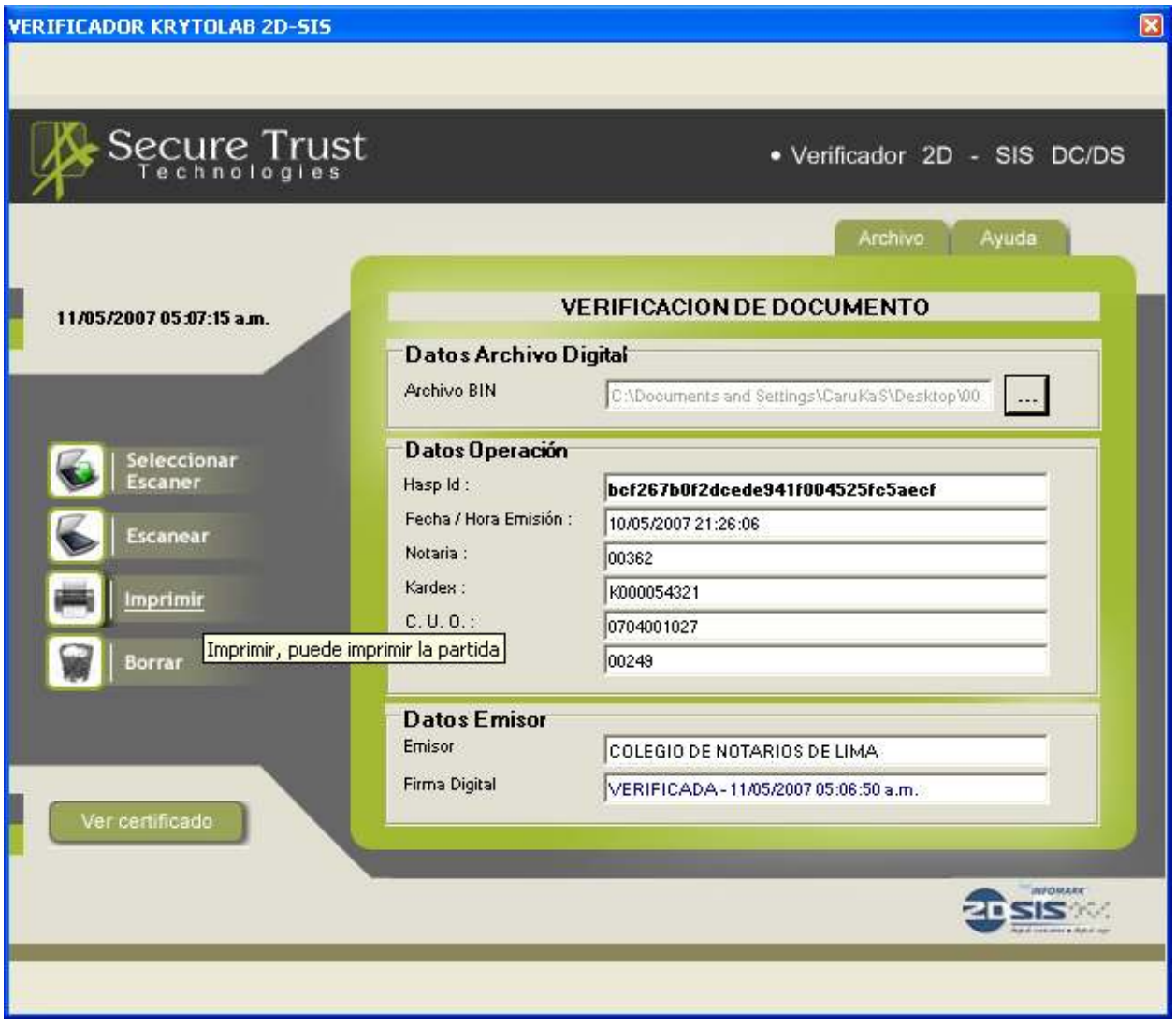
De lo contrario se cargará la ventana de previsualización del documento en el dispositivo externo (escáner)



Seleccionamos la región del código esteganográfico y hacemos clic en el botón Scan. La aplicación procederá a digitalizar y decriptar el código (previa verificación de la existencia de los certificados de la firma digital correspondientes, un público y un privado por ser cifrado asimétrico) para luego obtener los datos ocultos que permitirán obtener el campo llave (hash) con el cual hará el match con el archivo BIN precargado.

Si el match es correcto mostrará un mensaje de verificación completada:

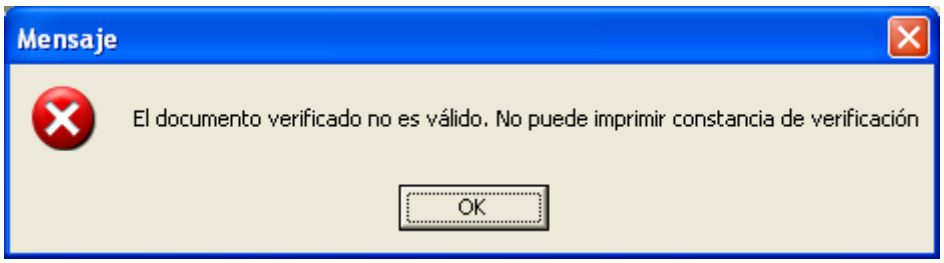
Luego procede a mostrar los datos descifrados en pantalla.



PROCESO IMPRIMIR

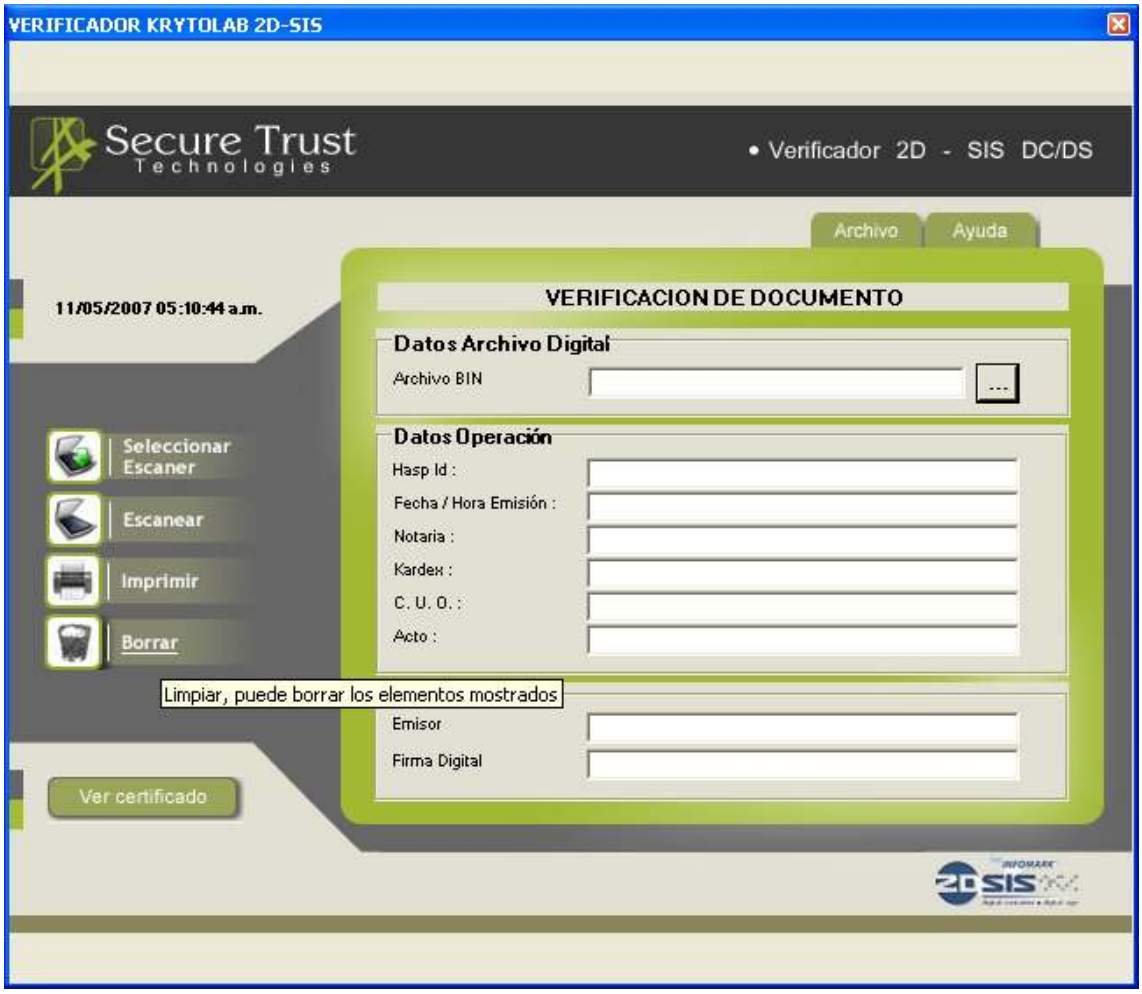
Este proceso nos permitirá emitir la constancia de verificación del documento en donde se muestran los datos obtenidos del código en el proceso de decriptación incluyendo la fecha y hora en que fue verificado.

En caso el proceso de verificación realizado al momento de escanear no haya sido satisfactorio no podrá imprimir esta constancia mostrando el siguiente mensaje de error:



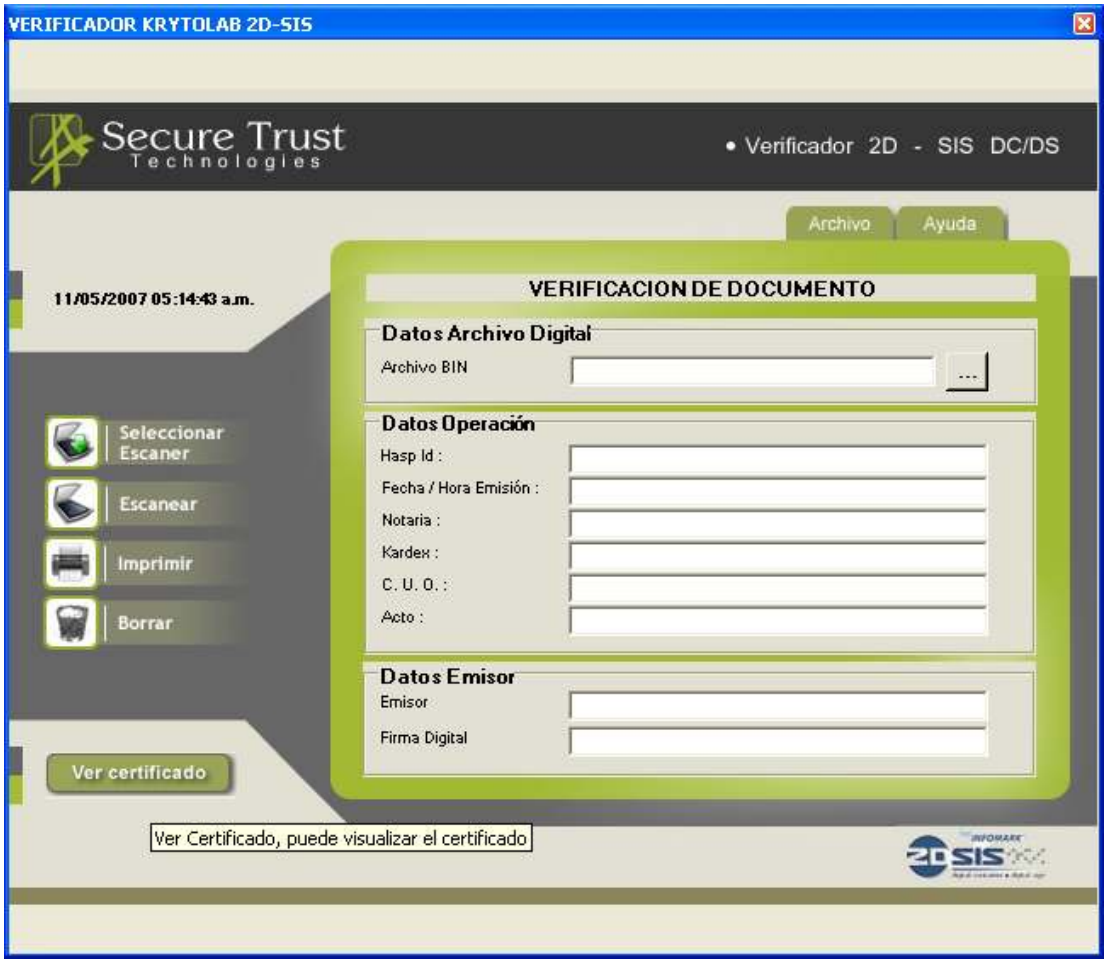
PROCESO BORRAR

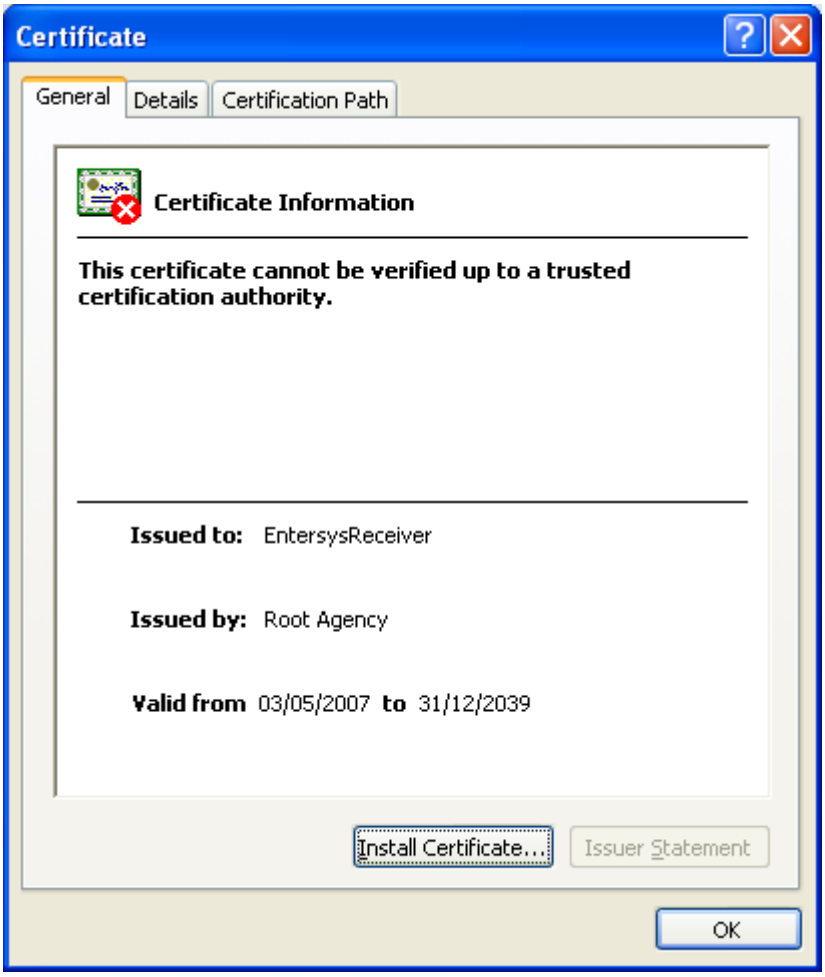
Este proceso nos permitirá limpiar la pantalla para iniciar una nueva verificación de documento.



VER CERTIFICADO

Muestra las propiedades del certificado digital en uso.




Certificate
General
Details
Certification Path
Certificate Information
This certificate cannot be verified up to a trusted certification authority.
Issued to: EntersysReceiver
Issued by: Root Agency
Valid from 03/05/2007 to 31/12/2039
Install Certificate...
Issuer Statement
OK

PARTE V - CONCLUSIONES

- Al tener un documento seguro desde su emisión hasta su inscripción en los registros públicos se logra minimizar el riesgo de la falsificación de los documentos a través de la infraestructura tecnológica utilizada (hardware y software).

- Garantizar la seguridad jurídica que es interés del Estado y el Colegio de Notarios de Lima en el ámbito de la normativa legal.

- Reducción de costos tanto para las notarias como para el ciudadano al eliminar los costos asociados al transporte y tramitadores, además de aquellos tramites que ya no son necesarios.

- Con el empleo de formatos preaprobados se logra minimizar las observaciones en el proceso registral, además de mostrar que es posible canalizar cualquier documento generado.

- Los tiempos de transacción y de colas se ven reducidos de 11 días hábiles a máximo 72 horas para la obtención del documento de constitución de empresas optimizando el tiempo del ciudadano y las partes involucradas en este proceso.

- Con el software de encriptación desarrollado se logra las transacciones de los documentos en su forma original únicamente desde la aplicación y por los responsables.

- Este software de encriptación incluye un modulo de generación y exportación de archivos digitalmente firmados permitiendo su envío por medios electrónicos.

- El software de verificación desarrollado utilizando la tecnología de firma digital, permite desencriptar y cotejar el contenido, verificando así el archivo digital enviado electrónicamente.

- Las características fundamentales de la tecnología de firma digital como son la autenticidad, integridad, no repudio y confidencialidad están plasmadas en el funcionamiento en conjunto de las aplicaciones de encriptación y verificación, que son parte del motivo de la tesis.

PARTE VI - REFERENCIAS BIBLIOGRAFICAS

[1] Borja, Lázaro de Rafael. Martinez-Ridruejo, Carlos del Cuvillo. Garcia Garcia, Héctor. Perez Donoso, Diego. Certificación de la Firma Digital. Editorial Forem. 2003.

[2] Caballero Gil, Pino. Introducción a la Criptografía. Editorial Ra-ma. 2002

[3] Oliver Pell. Cryptology.
http://www.ridex.co.uk/cryptology/

[4] General Purpose Hash Function Algorithms
http://www.partow.net/programming/hashfunctions/index.html

[5] RFC 1321 - The MD5 Message-Digest Algorithm
http://tools.ietf.org/html/rfc1321

[6] Electronic Frontier Foundation. Specifications for a SECURE HASH STANDARD (SHS)
http://w2.eff.org/Privacy/Digital_signature/?f=fips_sha_shs.standard.txt

[7] Bruce Schneir. Schneier on Security: Cryptanalysis of SHA-1
http://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html

[8] Chris Sells, Jon. Flanders, Ian Griffiths. Mastering Visual Studio .NET. Editorial O'Reilly. 2003.

[9] Jesse Liberty, Dan. Hurwitz. Programming .NET Windows Applications. Editorial O'Reilly. 2003.

[10] Austin, Tom. PKI: Planning and Implementing Digital Certificate Systems. Editorial Wiley. 2001.

[11] Larman, Craig. UML y Patrones: Introducción al Análisis y Diseño Orientado a Objetos. Editorial Prentice-Hall. 2006

[12] Erick Iriarte Ahon, "Firma Digital y Certificado Digital. El Proyecto Peruano", Revista Alpha- Redi No. 014 - Septiembre del 1999.

[13] Machado Jorge. "Parches De Sistemas Operativos Para Certificaciones Digitales", Publicado Miercoles 11 de Septiembre de 2002 en la Revista Tecnología sección software.

[14] Álvarez Marañon, Gonzalo. "SET a fondo Secure Electronic Transaction", iWORLD, Número: 22, Sección: Artículos, 12/1/1999.

[15] Ferrando Perea, Ivan. “Gobierno Electrónico: Nuevas disposiciones sobre firma digital en el ámbito de la Administración pública peruana”, Revista Alpha- Redi, No. 117 - Abril del 2008.

[16] Llopis Méndez, Josep. “Agència Catalana de Certificación: la certificación digital en la Administración Pública catalana”, Novática núm. 171, sep.-oct. 2004.

[17] Centre de Supercomputació de Catalunya. Certificados. http://www.cesca.es/es/comunicacions/scd/certificats.html

[18] Virginia Pérez Pino, “Carnet Colegial para Abogados”, La TOGA, Nº 157, Enero/Febrero 2006.

[19] Bustos P., Cristián. “Impacto de Factura Electrónica en PYMES”, Universidad DE Chile, Seminario para optar al título de Ingeniero Comercial, Santiago – Chile, 2003.

[20] Maulén Gálvez, Ignacio Javier. Santín Díaz, Christián Mauricio. Yang Li, Ching Chin. Universidad de Chile , “Firma Digital y D.T.E., Usos y Beneficios en Chile ”, Tesis para optar al título profesional de Ingeniero en Información y Control de Gestión y Contador Auditor, Santiago, Chile 2003.

[21] Tintó Gimbernat, Montserrat, Universitat Pompeau Fabra, “La Administración pública en la sociedad de la información: el régimen jurídico de la administración pública electrónica”, 10 de Diciembre del 2002

[22] Radbruch, Gustav. Introducción a la filosofía del derecho. México: FCE, 1993

[23] Kniberg, Henrik. Scrum and XP from the Trenches. Editorial Lulu.com. 2002

[24] Palacio, José. Flexibilidad con Scrum. Editorial Lulu.com. Noviembre 2007.

[25] Wallace, Doug. Raggett, Isobel. Aufgang, Joel. Extreme Programming for Web Projects. Editorial Addison Wesley. 2002.

[26] Beck, Kent. Extreme Programming Explained: Embrace Change. Editorial Addisson-Wesley. 2001

[27] Indecopi. “Firma y Certificación Digital”. http://www.indecopi.gob.pe/servicios-FirmaCerDigital-que-es.jsp.

[28] Hebrero Hernández, José Antonio. La firma digital. Derecho de las Nuevas Tecnologías. http://www.tuguialegal.com/firmadigital.htm.

[29] Infraestructura de clave pública (PKI) http://www.firmadigital.mendoza.gov.ar/sds/sds03.pdf

[30] Smart Card Alliance. About Smart Cards : Frequently Asked Questions http://www.smartcardalliance.org/pages/smart-cards-faq

[31] How does a Smart Card Reader work? TechFAQ. http://www.tech-faq.com/smart-card-reader.shtml

[32] Octavia Andreea Anghel. A Guide to Cryptography in PHP. http://www.devx.com/webdev/Article/37821.

[33] Guillermo Som. .NET Namespaces - System.Security.Cryptography. http://www.elguille.info/NET/library/System.Security.Cryptography.aspx

[34] Decreto Supremo Nº019-2007-PCM - Establecimiento de uso de la Ventanilla Única del Estado. http://www.pcm.gob.pe/Prensa/ActividadesPCM/2007/Marzo2007/DS-019-2007-PCM.pdf

[35] Bernal García, Juan Jesús. Martínez María Dolores, Soledad María. Sánchez García, Juan Francisco. Encriptación en la comunicación de información electrónica. Una propuesta didáctica. Universidad Politécnica de Cartagena. 2004. http://www.uv.es/asepuma/XII/comunica/bernal_martinez_sanchez_2.pdf.

[36] Xiaoyun Wang, Hongbo Yu. How to Break MD5 and Other Hash Functions. 2004. http://www.infosec.sdu.edu.cn/uploadfile/papers/How%20to%20Break%20MD5%20and%20Other%20Hash%20Functions.pdf

[37] Arjen Lenstra. Xiaoyun Wang. Benne de Weger. Colliding X.509 Certificates. 2005 http://eprint.iacr.org/2005/067

INDICE DE FIGURAS

2.1 Ejemplos de Encriptación..... 20

2.2.1 Criptografía Asimétrica 21

2.2.2 Criptografía Simétrica 23

2.4 Hashing.....25

2.5.1-1 Componentes .Net Framework.....28

2.5.1-2 Conjunto de Librería .Net 29

2.7.1 Portal de Acceso a la Ventanilla Única del Estado.....36

4.4.1 Modelo de Casos de Uso de Negocios 64

4.4.2 Diagrama de Paquetes.....65

4.4.3 Modelo de Casos de Uso Encriptar Documentos 67

4.4.4 Modelo de Casos de Uso Desencriptar Documentos 68

PARTE VIII - ANEXOS

- Ley de Firmas y Certificados Digitales. Ley Nº 27269. (Año 2000)

- Decreto Supremo Nº 019-2007-PCM. Se establece el uso de la Ventanilla Única del Estado a través del Portal de Servicios al Ciudadano y Empresas y se crea el Sistema Integrado de Servicios Públicos Virtuales.

- Nuevo Reglamento de la Ley de las Firmas y Certificados Digitales. D.S N° 004-2007-PCM. (Año 2007)

LEY Nº 27269

EL PRESIDENTE DE LA REPÚBLICA

POR CUANTO:

El Congreso de la República
ha dado la Ley siguiente:

EL CONGRESO DE LA REPÚBLICA;

Ha dado la Ley siguiente:

LEY DE FIRMAS Y CERTIFICADOS DIGITALES

Artículo 1°.- Objeto de la ley
La presente ley tiene por objeto regular la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad.

Entiéndase por firma electrónica a cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse o autenticar un documento cumpliendo todas o algunas de las funciones características de una firma manuscrita.

Artículo 2°.- Ámbito de aplicación
La presente ley se aplica a aquellas firmas electrónicas que, puestas sobre un mensaje de datos o añadidas o asociadas lógicamente a los mismos, puedan vincular e identificar al firmante, así como garantizar la autenticación e integridad de los documentos electrónicos.

DE LA FIRMA DIGITAL

Artículo 3°.- Firma digital
La firma digital es aquella firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada.

DEL TITULAR DE LA FIRMA DIGITAL

Artículo 4°.- Titular de la firma digital
El titular de la firma digital es la persona a la que se le atribuye de manera exclusiva un certificado digital que contiene una firma digital, identificándolo objetivamente en relación con el mensaje de datos.

Artículo 5°.- Obligaciones del titular de la firma digital
El titular de la firma digital tiene la obligación de brindar a las entidades de certificación y a los terceros con quienes se relacione a través de la utilización de la firma digital, declaraciones o manifestaciones materiales exactas y completas.

DE LOS CERTIFICADOS DIGITALES

Artículo 6°.- Certificado digital
El certificado digital es el documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula un par de claves con una persona determinada confirmando su identidad.

Artículo 7°.- Contenido del certificado digital
Los certificados digitales emitidos por las entidades de certificación deben contener al menos:

1. Datos que identifiquen indubitablemente al suscriptor.
2. Datos que identifiquen a la Entidad de Certificación.
3. La clave pública.
4. La metodología para verificar la firma digital del suscriptor impuesta a un mensaje de datos.
5. Número de serie del certificado.
6. Vigencia del certificado.
7. Firma digital de la Entidad de Certificación.

Artículo 8°.- Confidencialidad de la información
La entidad de registro recabará los datos personales del solicitante de la firma digital directamente de éste y para los fines señalados en la presente ley.

Asimismo la información relativa a las claves privadas y datos que no sean materia de certificación se mantiene bajo la reserva correspondiente. Sólo puede ser levantada por orden judicial o pedido expreso del suscriptor de la firma digital.

Artículo 9°.- Cancelación del certificado digital
La cancelación del certificado digital puede darse:

1. A solicitud del titular de la firma digital.
2. Por revocatoria de la entidad certificante.
3. Por expiración del plazo de vigencia.
4. Por cese de operaciones de la Entidad de Certificación.

Artículo 10°.- Revocación del certificado digital
La Entidad de Certificación revocará el certificado digital en los siguientes casos:

1. Se determine que la información contenida en el certificado digital es inexacta o ha sido modificada.
2. Por muerte del titular de la firma digital.
3. Por incumplimiento derivado de la relación contractual con la Entidad de Certificación.

Artículo 11°.- Reconocimiento de certificados emitidos por entidades extranjeras
Los Certificados de Firmas Digitales emitidos por entidades extranjeras tendrán la misma validez y eficacia jurídica reconocida en la presente ley, siempre y cuando tales certificados sean reconocidos por una entidad de certificación nacional que garantice, en la misma forma que lo hace con sus propios certificados, el cumplimiento de los requisitos, del procedimiento, así como la validez y la vigencia del certificado.

DE LAS ENTIDADES DE CERTIFICACIÓN Y DE REGISTRO

Artículo 12°.- Entidad de Certificación
La Entidad de Certificación cumple con la función de emitir o cancelar certificados digitales, así como brindar otros servicios inherentes al propio certificado o aquellos que brinden seguridad al sistema de certificados en particular o del comercio electrónico en general.

Las Entidades de Certificación podrán igualmente asumir las funciones de Entidades de Registro o Verificación.

Artículo 13°.- Entidad de Registro o Verificación
La Entidad de Registro o Verificación cumple con la función de levantamiento de datos y comprobación de la información de un solicitante de certificado digital; identificación y autenticación del suscriptor de firma digital; aceptación y autorización de solicitudes de emisión de certificados digitales; aceptación y autorización de las solicitudes de cancelación de certificados digitales.

Artículo 14°.- Depósito de los Certificados Digitales

Cada Entidad de Certificación debe contar con un Registro disponible en forma permanente, que servirá para constatar la clave pública de determinado certificado y no podrá ser usado para fines distintos a los estipulados en la presente ley.

El Registro contará con una sección referida a los certificados digitales que hayan sido emitidos y figurarán las circunstancias que afecten la cancelación o vigencia de los mismos, debiendo constar la fecha y hora de inicio y fecha y hora de finalización.

A dicho Registro podrá accederse por medios telemáticos y su contenido estará a disposición de las personas que lo soliciten.

Artículo 15°.- Inscripción de Entidades de Certificación y de Registro o Verificación

El Poder Ejecutivo, por Decreto Supremo, determinará la autoridad administrativa competente y señalará sus funciones y facultades.

La autoridad competente se encargará del Registro de Entidades de Certificación y Entidades de Registro o Verificación, las mismas que deberán cumplir con los estándares técnicos internacionales.

Los datos que contendrá el referido Registro deben cumplir principalmente con la función de identificar a las Entidades de Certificación y Entidades de Registro o Verificación.

Artículo 16°.- Reglamentación

El Poder Ejecutivo reglamentará la presente ley en un plazo de 60 (sesenta) días calendario, contados a partir de la vigencia de la presente ley.

DISPOSICIONES COMPLEMENTARIAS, TRANSITORIAS Y FINALES

Primera.- Mientras se cree el Registro señalado en el Artículo 15°, la validez de los actos celebrados por Entidades de Certificación y Entidades de Registro o Verificación, en el ámbito de la presente ley, está condicionada a la inscripción respectiva dentro de los 45 (cuarenta y cinco) días siguientes a la creación el referido Registro.

Segunda.- El Reglamento de la presente ley incluirá un glosario de términos referidos a esta ley y a las firmas electrónicas en general, observando las definiciones establecidas por los organismos internacionales de los que el Perú es parte.

Tercera.- La autoridad competente podrá aprobar la utilización de otras tecnologías de firmas electrónicas siempre que cumplan con los requisitos establecidos en la presente ley, debiendo establecer el Reglamento las disposiciones que sean necesarias para su adecuación.

Comuníquese al señor Presidente de la República para su promulgación.

En Lima, a los ocho días del mes de mayo del dos mil.

MARTHA HILDEBRANDT PÉREZ TREVIÑO
Presidenta del Congreso de la República

RICARDO MARCENARO FRERS
Primer Vicepresidente del Congreso de la República

AL SEÑOR PRESIDENTE CONSTITUCIONAL
DE LA REPÚBLICA

POR TANTO:

Mando se publique y cumpla.

Dado en la Casa de Gobierno, en Lima, a los veintiséis días del mes de mayo del año dos mil.

ALBERTO FUJIMORI FUJIMORI
Presidente Constitucional de la República

ALBERTO BUSTAMANTE BELAUNDE
Presidente del Consejo de Ministros y
Ministro de Justicia

AÑO DEL
DEBER CIUDADANO

El Peruano
DIARIO OFICIAL

FUNDADO
EN 1825 POR
EL LIBERTADOR
SIMÓN BOLÍVAR

Lima, viernes 9 de marzo de 2007

NORMAS LEGALES

Año XXIV - Nº 9765 www.elperuano.com.pe 341251

Sumario

PODER EJECUTIVO

PRESIDENCIA DEL CONSEJO DE MINISTROS

D.S. N° 019-2007-PCM.- Se establece el uso de la Ventanilla Única del Estado a través del Portal de Servicios al Ciudadano y Empresas y se crea el Sistema Integrado de Servicios Públicos Virtuales **341254**

R.S. N° 047-2007-PCM.- Autorizan viaje de la Ministra de Trabajo y Promoción del Empleo a EE.UU. y encargan su Despacho al Ministro de Agricultura **341255**

R.S. N° 048-2007-PCM.- Autorizan viaje de la Ministra de Transportes y Comunicaciones a Australia y encargan su Despacho al Ministro de Vivienda, Construcción y Saneamiento **341256**

R.M. Nº 071-2007-PCM.- Modifican TUPA del INDECI suprimiendo pago de derechos de trámite por interposición de recursos impugnativos **341256**

R.M. N° 078-2007-PCM.- Designan Director Ejecutivo del Programa Nacional de Apoyo Directo a los Más Pobres - JUNTOS **341257**

AGRICULTURA

R.M. N° 173-2007-AG.- Aprueban donación efectuada a favor de CARE PERÚ para proyecto de mejoramiento genético de ganadería **341257**

R.M. N° 219-2007-AG.- Designan Asesor de la Dirección Ejecutiva del Proyecto Especial Titulación de Tierras y Catastro Rural - PETT **341258**

R.M. N° 220-2007-AG.- Designan Jefes de las Oficinas PETT de Ejecución Regional de Madre de Dios y Ucayali **341258**

R.M. N° 222-2007-AG.- Designan Gerente Departamental de Ancash del PRONAMACHCS **341258**

R.M. N° 223-2007-AG.- Designan representante del Ministerio ante el Consejo Directivo del Proyecto Especial Olmos Tinajones del Gobierno Regional de Lambayeque **341259**

R.M. N° 226-2007-AG.- Designan responsables suplentes para el manejo de cuentas bancarias del PRONAMACHCS **341259**

COMERCIO EXTERIOR Y TURISMO

RR.SS. N°s. 039 y 040-2007-MINCETUR.- Autorizan viaje de representantes de PROMPEX para participar en eventos de organizaciones de promoción comercial que se realizarán en Argentina y en la Misión Empresarial a Colombia **341260**

R.M. N° 051-2007-MINCETUR/DM.- Designan representantes del Ministerio, PROMPERÚ y PROMPEX ante Comisión creada mediante D.S. N° 003-2007-MINCETUR **341261**

R.M. N° 053-2007-MINCETUR/DM.- Aprueban realización del Tercer Concurso Nacional de Tesis Universitarias, el Segundo Concurso Nacional de Proyectos Universitarios y el Primer Concurso Nacional de Proyectos Escolares **341261**

DEFENSA

R.S. N° 046-2007-DE/SG.- Autorizan viaje de oficial de la Marina de Guerra a Alemania para participar en el Curso de Observadores Militares de las Naciones Unidas - UNMOC **341262**

EDUCACION

R.M. N° 0113-2007-ED.- Aprueban "Normas que regulan el otorgamiento de licencias sindicales de los docentes de educación básica del Sector Educación a nivel Nacional" **341262**

R.M. N° 0114-2007-ED.- Declaran improcedente ampliación de Licencia de Representación Sindical a tiempo completo solicitada por el SUTEP y disponen la reincorporación inmediata de docentes a sus respectivas Instituciones Educativas **341263**

INTERIOR

R.S. N° 0021-2007-IN.- Encargan funciones de Viceministra del Interior a la Secretaria General del Ministerio **341264**

R.M. N° 155-2007-IN/0101.- Designan Jefe de Comité de Asesores del Despacho Ministerial **341264**

R.M. N° 156-2007-IN/0101.- Designan Asesor del Comité de Asesoramiento del Despacho Ministerial **341264**

MUJER Y DESARROLLO SOCIAL

R.M. N° 112-2007-MIMDES.- Aprueban reubicación laboral directa de ex trabajadores a la Unidad Ejecutora FONCODES **341265**

PRODUCE

R.S. N° 006-2007-PRODUCE.- Aceptan renuncia y designan Miembros del Consejo Directivo del Centro de Entrenamiento Pesquero de Paita - CEP PAITA **341265**

RR.VMS. Nºs. 009 y 010-2007-PRODUCE/DVP.- Declaran inadmisibles recursos de apelación interpuestos contra silencios administrativos negativos que habrían operado respecto a escritos presentados ante la Dirección Regional de Producción de Piura, sobre permiso de pesca **341266**

PODER EJECUTIVO

PRESIDENCIA DEL CONSEJO DE MINISTROS

Se establece el uso de la Ventanilla Única del Estado a través del Portal de Servicios al Ciudadano y Empresas y se crea el Sistema Integrado de Servicios Públicos Virtuales

DECRETO SUPREMO Nº 019-2007-PCM

EL PRESIDENTE DE LA REPÚBLICA

CONSIDERANDO:

Que, mediante la Ley Nº 27658, Ley Marco de Modernización de la Gestión del Estado, se declara al Estado Peruano en proceso de modernización en sus diferentes instancias, dependencias, entidades, organizaciones y procedimientos, con la finalidad de mejorar la gestión pública y contribuir en el fortalecimiento de un Estado moderno, descentralizado y con mayor participación del ciudadano; obteniendo mayores niveles de eficiencia del aparato estatal, de manera que se logre una mejor atención a la ciudadanía, priorizando y optimizando el uso de los recursos públicos;

Que, el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado mediante Decreto Supremo Nº 094-2005-PCM, establece que dicha Entidad es el ente rector del Sistema Nacional de Informática y que su Oficina Nacional de Gobierno Electrónico e Informática - ONGEI tiene la función de coordinar y supervisar el desarrollo de los portales de las entidades de la Administración Pública para facilitar la interrelación de las entidades entre sí y de éstas con el ciudadano con el fin de establecer la ventanilla única de atención, siendo responsable de coordinar y supervisar la integración funcional de los sistemas informáticos del Estado;

Que, el Desarrollo de la Plataforma de Red Transaccional del Estado y la Promoción e Implementación de un Sistema de Portales institucionales, adscritos al Portal del Estado Peruano son acciones incluidas en la matriz del Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana, aprobado por Decreto Supremo Nº 031-2006-PCM;

Que, a la fecha, diferentes entidades del sector público vienen realizando iniciativas sobre la implementación de Ventanillas Únicas, por lo cual resulta necesario que la Presidencia del Consejo de Ministros, como ente rector del Sistema Informático Nacional, unifique y reglamente su uso en el Perú a través del Portal de Servicios al Ciudadano y Empresas - PSCE;

Que, de otro lado, resulta necesario establecer un Sistema de información e interconexión que facilite y simplifique a los ciudadanos el acceso a los servicios públicos a través de la integración funcional e intercambio de tecnologías de información entre las entidades involucradas, lo cual disminuirá los tiempos en los servicios brindados;

En uso de las facultades conferidas por el numeral 8 del artículo 118º de la Constitución Política del Perú, el Decreto Supremo Nº 094-2005-PCM y el Decreto Supremo Nº 031-2006-PCM;

DECRETA:

Artículo 1º. - Uso de la Ventanilla Única del Estado

Establézcase el uso de la Ventanilla Única del Estado a través del Portal de Servicios al Ciudadano y Empresas - PSCE (www.serviciosalciudadano.gob.pe) adscrito al Portal del Estado Peruano - PEP de la Presidencia del Consejo de Ministros como la herramienta a través de la cual se brindan servicios públicos virtuales que ofrezcan las entidades de la Administración Pública.

Todas las entidades de la Administración Pública brindarán sus servicios virtuales mediante la Ventanilla Única del Estado desde la cual podrán vincularse a sus respectivas páginas web y a los consiguientes servicios que en ella se ofrezcan.

Artículo 2º. - Sistema Integrado de Servicios Públicos Virtuales

2.1. Créase el Sistema Integrado de Servicios Públicos Virtuales - SISEV como plataforma que permitirá a los ciudadanos acceder a los servicios públicos sectoriales y a los servicios públicos vinculados a éstos, que se brindan de manera virtual.

Se accede al Sistema Integrado de Servicios Públicos Virtuales - SISEV mediante la Ventanilla Única del Estado.

2.2. El Sistema Integrado de Servicios Públicos Virtuales - SISEV se encuentra conformado por los servicios públicos virtuales sectoriales que brindan dos o más entidades públicas, los que deberán ser adscritos al Portal de Servicios al Ciudadano y Empresas.

2.3. Mediante Resolución Ministerial de la Presidencia del Consejo de Ministros:

- Se autoriza a las entidades que así lo soliciten, que sus servicios públicos virtuales conformen el Sistema Integrado de Servicios Públicos Virtuales - SISEV; y,
- Se adscriben dichos servicios públicos virtuales sectoriales al Portal de Servicios al Ciudadano y Empresas.

2.4. Las entidades cuyos servicios públicos virtuales sectoriales se autoricen para conformar el Sistema Integrado de Servicios Públicos Virtuales - SISEV emitirán las disposiciones correspondientes y/o adoptarán las acciones necesarias para su cumplimiento y ejecución.

Artículo 3º.- Refrendo

El presente Decreto Supremo será refrendado por el Presidente del Consejo de Ministros.

DISPOSICIONES COMPLEMENTARIAS TRANSITORIAS

Primera.- Autorícese la participación de los servicios públicos que brindan el Registro Nacional de Identificación y Estado Civil (RENIEC), el Colegio de Notarios de Lima, la Superintendencia Nacional de los Registros Públicos (SUNARP), la Superintendencia Nacional de Administración Tributaria (SUNAT), el Ministerio de Trabajo y Promoción del Empleo - MTPE y la Agencia de Promoción de la Inversión Privada - PROINVERSIÓN al Sistema Integrado de Servicios Públicos Virtuales - SISEV.

Para su participación, estas entidades deberán cumplir con las acciones señaladas en el numeral 2.4 del artículo 2º del presente Decreto Supremo.

Segunda.- El primer servicio a implementarse bajo la plataforma del Sistema Integrado de Servicios Públicos Virtuales - SISEV será el de constitución de empresas, el mismo que incluirá tanto la inscripción en los Registros Públicos correspondiente como el otorgamiento del número del Registro Único del Contribuyente.

Este servicio estará inicialmente a disposición de los usuarios en la ciudad de Lima Metropolitana, implementándose progresivamente en el resto del país.

Las entidades autorizadas a que se refiere la Primera Disposición Complementaria Transitoria, y que se encuentran involucradas en el servicio de constitución de empresas, dictarán las disposiciones correspondientes y/o adoptarán las acciones necesarias para la puesta en marcha del servicio, en un plazo de diez (10) días calendario contados a partir del día siguiente a la publicación del presente Decreto Supremo.

Culminado el plazo previsto en el párrafo anterior, se podrá acceder al servicio de constitución de empresas, en el que participarán los Notarios de Lima propuestos por el Colegio de Notarios de Lima según la relación que se detalla en el anexo que forma parte del presente Decreto Supremo.

Tercera.- Incorpórense a la Ventanilla Única del Estado aquellos servicios públicos virtuales sectoriales constituidos a la fecha, independientemente de su denominación.

Cuarta.- La Presidencia del Consejo de Ministros elaborará las disposiciones reglamentarias y complementarias que sean necesarias.

Dado en la Casa de Gobierno, en Lima a los ocho días del mes de marzo del año dos mil siete.

ALAN GARCÍA PÉREZ
Presidente Constitucional de la República

JORGE DEL CASTILLO GÁLVEZ
Presidente del Consejo de Ministros

ANEXO

	RELACIÓN DE NOTARIOS
1	Alberti Sierra, Renzo
2	Banda González, Francisco
3	Bazán Naveda, César
4	Berrospi Polo, Sergio A.
5	Canelo Ramírez, Wilson
6	Carnero Avalos, Clara P.

	RELACIÓN DE NOTARIOS
7	Chuquiure Valenzuela, María
8	Diaz Delgado, Roque
9	Espinosa-Garreta, Ramón
10	Espinosa Ore, Aldo Ramón
11	Fernandini Barreda, Ricardo
12	González Bazán, Arnaldo
13	Gonzalez Loli, Jorge Luis
14	Gonzalez-Vigil Balbuena, Percy
15	Herrera Portuondo, Isabel Bárbara
16	Hidalgo Morán, C. Cecilia
17	Higa Nakamura, Isaac
18	Landazuri Golffer, Cyra Ana
19	Laos de Lama, Eduardo
20	Marin Portocarrero, Rebeca Lizbet
21	Mejia Rosasco, Rosalia
22	Montoya Romero, Fausto
23	Ortiz de Zevallos Villarán, Ricardo
24	Paino Scarpati, José Alfredo
25	Peralta Castellano, Juan Carlos
26	Ramos Rivas, Ruth Alessandra
27	Romero Valdivieso, Mario César
28	Salgado Padilla, A. Felipe
29	Salvatierra Saldaña, Monica
30	Sanchez Manrique Tavella, David
31	Sekula Delgado, Ljubica N.
32	Sotero Villar, Getrudes
33	Sotomayor Bernos, Carlos Augusto
34	Tambini Avila, Mónica
35	Torres Zevallos, Fidel D'Jalma
36	Tuccio Valverde, Jaime
37	Vidal Hermoza, Ana María
38	Yáñez Aspilcueta, Loudelvi
39	Zevallos Giampietri, Beatriz

34750-1

Autorizan viaje de la Ministra de Trabajo y Promoción del Empleo a EE.UU. y encargan su Despacho al Ministro de Agricultura

RESOLUCIÓN SUPREMA
Nº 047-2007-PCM

Lima, 8 de marzo de 2007

VISTO: El Memorando Nº 277-2007-MTPE/4 de fecha 6 de marzo de 2007, del Secretario General del Ministerio de Trabajo y Promoción del Empleo; y,

CONSIDERANDO:

Que, la suscripción del Tratado de Libre Comercio - TLC entre el Gobierno Peruano con el Gobierno de los Estados Unidos, permitirá que nuestro país tenga acceso a un mercado de mayor capacidad adquisitiva, mejores y nuevas inversiones, leyes arancelarias claras, posicionamiento estratégico, competitividad y más puestos de trabajo;

Que, siendo prioridad del Estado Peruano la aprobación de dicho Tratado, resulta conveniente autorizar el viaje de la señora Ministra de Trabajo y Promoción del Empleo a la ciudad de Washington D.C., Estados Unidos de Norteamérica, a fin de que los días 12 y 13 de marzo de 2007, sostenga reuniones de trabajo con autoridades del Congreso y del Gobierno de dicho país, para fortalecer la posición peruana sobre la conveniencia de la firma del Tratado de Libre Comercio - TLC;

Que, en tal sentido, considerando que las referidas reuniones se enmarcan dentro de los objetivos y metas indispensables del Sector Trabajo y Promoción del Empleo, resulta conveniente autorizar el viaje de la señora Susana Isabel Pinilla Cisneros, Ministra de Trabajo y Promoción del Empleo, encargándose además, la Cartera de Trabajo y Promoción del Empleo al Ministro de Agricultura, quien la reemplazará;

Con la visación de la Directora General (e) de la Oficina de Asesoría Jurídica; y,

Artículo 28°.- Reglamento del Consejo de Usuarios

El Consejo de Usuarios se rige en su funcionamiento por el Reglamento que aprueba el Consejo Directiva del Organismo Regulador, a propuesta del primer Consejo de Usuarios que se instale en virtud de la Primera Disposición Transitoria del presente Decreto Supremo.

El Reglamento del Consejo de Usuarios incorporará disposiciones para la elección del Coordinador.

El Consejo de Usuarios tiene iniciativa para proponer a Consejo Directivo del Organismo Regulador, mediante solicitud debidamente fundamentada, la modificación del reglamento del Consejo de Usuarios."

Artículo 2°.- Del refrendo

El presente Decreto Supremo será refrendado por el Presidente del Consejo de Ministros.

Dado en la casa de Gobierno, en Lima, a los doce días del mes de enero del año dos mil siete.

ALAN GARCÍA PÉREZ
Presidente Constitucional de la República

JORGE DEL CASTILLO GÁLVEZ
Presidente del Consejo de Ministros

15539-13

Aprueba Reglamento de la Ley de Firmas y Certificados Digitales

DECRETO SUPREMO
N° 004-2007-PCM

EL PRESIDENTE DE LA REPÚBLICA

CONSIDERANDO:

Que, mediante Ley N° 27269 - Ley de Firmas y Certificados Digitales, modificada por la Ley N° 27310, se reguló la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga, en especial la utilización de la firma digital y los certificados digitales; se reguló a las entidades de certificación y de registro, y se estableció que el Poder Ejecutivo, por Decreto Supremo, determinaría la autoridad administrativa competente y señalaría sus funciones y facultades;

Que, mediante el Decreto Supremo N° 019-2002-JUS, modificado por el Decreto Supremo N° 024-2002-JUS, se aprobó el Reglamento de la Ley N° 27269 - Ley de Firmas y Certificados Digitales, y se designó al Instituto Nacional de Defensa de la Competencia y la Protección de la Propiedad Intelectual (INDECOPI) como la Autoridad Administrativa Competente, encargada de administrar la Infraestructura Oficial de Firma Electrónica - IOFE;

Que, mediante Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado, se declara al Estado Peruano en proceso de modernización en sus diferentes instancias y procedimientos, con la finalidad de mejorar la gestión pública y contribuir en el fortalecimiento de un Estado moderno, descentralizado y con mayor participación del ciudadano, siendo necesario impulsar la Infraestructura Oficial de Firma Electrónica - IOFE;

Que conforme a la Ley N° 26497, Ley Orgánica del Registro Nacional de Identificación y Estado Civil - RENIEC, corresponde al RENIEC planear, dirigir, coordinar y controlar las actividades de registro e identificación de las personas, así como emitir el documento único que acredita la identidad de las personas.

Que, la Ley N° 27444 - Ley del Procedimiento Administrativo General establece entre las modalidades de notificación, las cursadas mediante correo electrónico; asimismo permite la cancelación de los derechos de tramitación mediante transferencias electrónicas de fondos; y, que los administrados puedan solicitar que el envío de información o documentación que les corresponda recibir dentro de un procedimiento, sea realizado por medios de transmisión a distancia, tales como el correo electrónico;

Que, el numeral 28.4 del artículo 28° de la precitada Ley N° 27444, prevé que la constancia documental de la transmisión a distancia por medios electrónicos entre entidades y autoridades, constituye de por sí documentación auténtica y dará plena fe a todos sus efectos dentro del expediente para ambas partes, en cuanto a la existencia del original transmitido y su recepción;

Que, en consecuencia, es pertinente aprobar un nuevo Reglamento de la Ley N° 27269 - Ley de Firmas y Certificados Digitales, que permitirá poner en práctica y difundir en el más breve plazo el uso de firmas electrónicas y certificados digitales, a través de la adecuada regulación de las entidades de certificación y de las entidades de registro o verificación, tanto en el sector público como en el sector privado, impulsando el desarrollo del Comercio y del Gobierno Electrónico, así como de la Sociedad de la Información;

Que, la Presidencia del Consejo de Ministros es la instancia encargada de coordinar esfuerzos intersectoriales para desarrollar el proceso de modernización de la gestión pública; asimismo, de conformidad con el Decreto Supremo N° 066-2003-PCM y el artículo 34° del Decreto Supremo N° 094-2005-PCM, la Presidencia del Consejo de Ministros, actúa como ente rector del Sistema Nacional de Informática;

Con la opinión favorable de la Secretaría de Gestión Pública de la Presidencia del Consejo de Ministros y de la RENIEC contenida en el Oficio N° 997-2006/SGEN/RENIEC;

De conformidad con lo dispuesto en el inciso 8) del artículo 118° de la Constitución Política del Perú, el inciso 2) del artículo 3° del Decreto Legislativo N° 560, la Ley N° 27269 - Ley de Firmas y Certificados Digitales, la Ley N° 28403 y el Decreto Ley N° 25868;

DECRETA:

Artículo 1°.- Aprobación

Apruébese el Reglamento de la Ley N° 27269 - Ley de Firmas y Certificados Digitales, modificada por la Ley N° 27310, que consta de tres (3) Títulos, cincuenta y ocho (58) Artículos y Ocho (8) Disposiciones Finales, que en Anexo forma parte del presente Decreto Supremo.

Artículo 2°.- Derogación

Deróguese el Decreto Supremo N° 019-2002-JUS y el Decreto Supremo N° 024-2002-JUS.

Artículo 3°.- Refrendo

El presente Decreto Supremo será refrendado por el Presidente del Consejo de Ministros.

Dado en la Casa de Gobierno, a los doce días del mes de enero del año dos mil siete.

ALAN GARCÍA PÉREZ
Presidente Constitucional de la República

JORGE DEL CASTILLO GÁLVEZ
Presidente del Consejo de Ministros

REGLAMENTO DE LA LEY DE FIRMAS Y CERTIFICADOS DIGITALES

TÍTULO I

DISPOSICIONES GENERALES

Artículo 1°.- Objeto

El objeto de la presente norma es regular, para el sector público y privado, la utilización de las firmas electrónicas y el régimen de la Infraestructura Oficial de Firma Electrónica

(IOFE), que comprende la acreditación y supervisión de las entidades de certificación y de las entidades de registro o verificación; de acuerdo a lo establecido en la Ley Nº 27269- Ley de Firmas y Certificados Digitales en adelante la Ley.

Reconociendo la variedad de las modalidades de firmas electrónicas, la diversidad de garantías que ofrecen, los diversos niveles de seguridad y la heterogeneidad de las necesidades de sus potenciales usuarios, la IOFE no excluye ninguna modalidad, ni combinación de modalidades de firmas electrónicas conforme a los requisitos establecidos en el artículo 2º de la Ley.

Artículo 2º.- Utilización de las Firmas Electrónicas

Las disposiciones contenidas en el presente Reglamento no restringen la utilización de las firmas electrónicas generadas fuera de la IOFE, las cuales serán válidas en consideración a los pactos o convenios que acuerden las partes, así como las políticas que adopte el Estado sobre la validez y eficacia jurídica de la firma electrónica en la Administración Pública, conforme a lo establecido en el artículo 1º de la Ley.

Artículo 3º.- Régimen de servicios de certificación

La prestación de servicios de certificación, así como los de registro o verificación, en el ámbito del sector privado se sustentan en el principio de libre competencia.

CAPÍTULO I

DE LA VALIDEZ Y EFICACIA JURÍDICA DE LAS FIRMAS Y DOCUMENTOS ELECTRÓNICOS

Artículo 4º.- Firma electrónica

Se entenderá por firma electrónica a cualquier símbolo basado en medios electrónicos, generado dentro o fuera de la IOFE, utilizado o adoptado por una parte con la intención precisa de vincularse, autenticar y/o garantizar la integridad de un documento electrónico o un mensaje de datos cumpliendo todas o algunas de las funciones características de una firma manuscrita.

Artículo 5º.- Validez y eficacia de las firmas electrónicas

La firma digital generada dentro de la IOFE tiene la misma validez y eficacia jurídica que el uso de una firma manuscrita. En tal sentido, cuando la ley exija la firma de una persona, ese requisito se entenderá cumplido en relación con un mensaje de datos o documento electrónico si se utiliza una firma digital generada en el marco de la IOFE.

A las firmas electrónicas creadas o utilizadas fuera de la IOFE, no se le negarán efectos jurídicos, su validez está sometida a los acuerdos o convenios entre las partes, como también a las disposiciones legales aprobadas por el Estado en el marco de las políticas sobre validez de la firma electrónica en el ámbito de la Administración Pública.

CONSUCODE
Consejo Superior de Contrataciones y Adquisiciones del Estado

RESULTADO DEL PROCESO DE FISCALIZACIÓN POSTERIOR PERÍODO DICIEMBRE - 2006

Nº	CONTRATISTA	Nº REG.	Nº RESOLUCION (*)	SUMILLA DE RESOLUCION
1	ROYJA INGENIEROS S.R.L.	8633	Resolución de Subgerencia Nº 017-2006-CONSUCODE/GRNP/SFP del 18.12.2006	Por no comunicar oportunamente la variación de su plantel técnico, se **cancela** la vigencia de la inscripción otorgada a la empresa mediante Resolución de Subgerencia Nº -1234-2006 de fecha 07.08.2006 y se deja sin efecto legal el Certificado de Inscripción Nº 1440 de fecha 08.08.2006.
2	FODERECA E.I.R.L.	11153	Resolución de Presidencia Nº 518-2006-CONSUCODE/PRE del 17.11.2006.	Disponer el inicio de las acciones legales, vía proceso contencioso administrativo, a fin de que en sede judicial se declarare la nulidad de la Resolución de Gerencia Nº 1262-2005-CONSUCODE/GR de fecha 27.07.2005, que aprobó la Inscripción en el Registro Nacional de Proveedores, poner en conocimiento del Ministerio Público, la presunta comisión de los delitos contra la función jurisdiccional (falsa declaración en procedimiento administrativo y contra la fe pública en agravio de CONSUCODE, poner este hecho en conocimiento del Tribunal de Contrataciones y Adquisiciones del Estado, para iniciar el procedimiento sancionador a que hubiere lugar.
3	ARQUITECTURA CONSTRUCCIONES SERVICIOS ANEXOS S.R.L. (ACSA S.R.L.)	4521	Resolución de Presidencia Nº 528-2006-CONSUCODE/PRE del 24.11.2006.	Disponer el inicio de las acciones legales, vía proceso contencioso administrativo, a fin de que en sede judicial se declarare la nulidad de la Resolución de Gerencia Nº 1736-2005-CONSUCODE/GR de fecha 27.09.2005, que aprobó la Renovación de Inscripción en el Registro Nacional de Proveedores, poner en conocimiento del Ministerio Público, la presunta comisión de los delitos contra la función jurisdiccional (falsa declaración en procedimiento administrativo y contra la fe pública en agravio de CONSUCODE, poner este hecho en conocimiento del Tribunal de Contrataciones y Adquisiciones del Estado, para iniciar el procedimiento sancionador a que hubiere lugar.
4	TYON E.I.R.L.	5469	Resolución de Presidencia Nº 529-2006-CONSUCODE/PRE del 24.11.2006.	Disponer el inicio de las acciones legales, vía proceso contencioso administrativo, a fin de que en sede judicial se declarare la nulidad de la Resolución de Gerencia Nº 1887-2005-CONSUCODE/GR de fecha 17.10.2005, que aprobó la Renovación de Inscripción en el Registro Nacional de Proveedores, disponer el inicio de las acciones legales contra el representante legal de la empresa por la presunta comisión de los delitos contra la función jurisdiccional (falsa declaración en procedimiento administrativo) en agravio de CONSUCODE, poner este hecho en conocimiento del Tribunal de Contrataciones y Adquisiciones del Estado para iniciar el procedimiento sancionador a que hubiere lugar.

Lima, enero de 2006
Gerencia de Registros

Lo establecido en el presente artículo y las demás disposiciones del presente Reglamento no excluyen el cumplimiento de las formalidades específicas requeridas para los actos jurídicos y el otorgamiento de fe pública.

Artículo 6°.- Documentos Firmados Electrónicamente como medio de prueba

Los mensajes de datos y los documentos firmados electrónicamente deberán ser admitidos como prueba en los procesos judiciales y/o procedimientos administrativos. Esto incluye la posibilidad de que a voluntad de las partes puede haberse utilizado un servicio de intermediación electrónica.

El Juez podrá solicitar a la AAC el nombramiento de un perito especializado en firmas electrónicas.

Artículo 7°.- Tecnologías de firmas electrónicas

Las firmas electrónicas podrán basarse en todas las tecnologías disponibles de acuerdo con el principio de neutralidad tecnológica. La Infraestructura Oficial de Firma Electrónica admitirá todas las tecnologías de firma digital acreditadas por la AAC.

Artículo 8°.- Conservación de mensaje de datos o documentos electrónicos

Cuando los documentos, registros o informaciones requieran de una formalidad adicional para la conservación de mensajes de datos o documentos electrónicos firmados electrónicamente, deberán:

a) Ser accesibles para su posterior consulta.

b) Ser conservados con su formato original de generación, envío, recepción u otro formato que reproduzca en forma demostrable la exactitud e integridad del contenido electrónico.

c) Ser conservado todo dato que permita determinar el origen, destino, fecha y hora del envío y recepción.

TÍTULO II

DE LA INFRAESTRUCTURA OFICIAL DE FIRMA ELECTRÓNICA

CAPÍTULO I
ASPECTOS GENERALES

Artículo 9°.- Elementos

La Infraestructura Oficial de Firma Electrónica - IOFE - está constituida por:

a) El conjunto de firmas electrónicas, certificados digitales y documentos electrónicos generados bajo la Infraestructura Oficial de Firma Electrónica.

b) Las prácticas de certificación, basadas en estándares internacionales o compatibles a las internacionalmente vigentes, que aseguren la interoperabilidad y las funciones exigidas, conforme a lo establecido por la AAC.

c) El software, el hardware y demás componentes adecuados para las prácticas de certificación y las condiciones de seguridad adicionales comprendidas en los estándares señalados en el inciso b).

d) Sistema de gestión que permita el mantenimiento de las condiciones señaladas en los literales anteriores, así como la seguridad, confidencialidad, transparencia y no discriminación en la prestación de sus servicios.

e) La AAC, así como Entidades de Certificación, Entidades de Registro o Verificación, Entidad de Certificación Nacional para el Estado Peruano (ECERNEP), Entidades de Certificación para el Estado Peruano (ECEP) y Entidades de Registro o Verificación para el Estado Peruano (EREP), debidamente acreditadas o reconocidas.

Artículo 10°.- Estándares aplicables

La AAC determinará los estándares compatibles aplicando el principio de neutralidad tecnológica.

CAPÍTULO II
DE LAS ENTIDADES DE CERTIFICACIÓN

Artículo 11°.- Funciones

Las Entidades de Certificación tendrán las siguientes funciones:

a) Emitir certificados digitales manteniendo su numeración correlativa.

b) Cancelar certificados digitales.

c) Reconocer certificados digitales emitidos en el extranjero y responder por ellos.

d) Adicionalmente a las anteriores, las señaladas en el artículo 15° del Reglamento, en caso opten por asumir las funciones de Entidad de Registro o Verificación.

Las Entidades de Certificación podrán brindar otros servicios inherentes a los de certificación, cuyas características y procedimientos estarán contenidos en su declaración de prácticas de certificación.

Artículo 12°.- Obligaciones

Las Entidades de Certificación registradas tienen las siguientes obligaciones:

a) Cumplir con su Declaración de Prácticas de Certificación.

b) Cumplir sus funciones dentro de los plazos señalados en su Declaración de Prácticas de Certificación.

c) Informar a los usuarios de todas las condiciones de emisión y de uso de sus certificados digitales, incluyendo las referidas a la cancelación de éstos.

d) Mantener el control y la reserva de la clave privada que emplea para firmar los certificados digitales que emite. En caso que la clave privada de la entidad de certificación se vea comprometida, de inmediato la entidad de certificación cancelará públicamente todos los certificados que haya emitido, u otra medida que haya sido determinada por la AAC.

e) Mantener depósito de los certificados digitales emitidos y cancelados, consignando su fecha de emisión y vigencia.

f) Publicar permanente e ininterrumpidamente por medios telemáticos la relación de los certificados digitales emitidos y cancelados.

g) Cancelar el certificado digital a solicitud de su titular o, de ser el caso, a solicitud del titular de la firma digital; o cuando advierta que la información contenida en el certificado digital fuera inexacta o hubiera sido modificada, o que el titular incurriera en alguna de las causales previstas en el artículo 30° del Reglamento.

h) Mantener la confidencialidad de la información relativa a los solicitantes y titulares de certificados digitales limitando su empleo a las necesidades propias del servicio de certificación, salvo orden judicial o pedido expreso del titular del certificado digital.

i) Brindar todas las facilidades al personal autorizado por la AAC para efectos de supervisión y auditoría.

j) Mantener la información relativa a los certificados digitales que hubieren sido cancelados, por un período mínimo de diez (10) años a partir de su cancelación.

k) Cumplir los términos bajo los cuales obtuvo la acreditación, así como los requerimientos adicionales que establezca la AAC conforme a lo establecido en el Reglamento.

l) Informar y solicitar autorización a la AAC para realizar acuerdos de certificación cruzada que proyecte celebrar, así como los términos bajo los cuales dichos acuerdos se suscribirían.

m) Informar y solicitar autorización a la AAC para efectos del reconocimiento de certificados emitidos por entidades extranjeras.

n) Mantener vigente la contratación de seguros o garantías bancarias que permitan indemnizar al titular por los daños que puedan ocasionar como resultado de las actividades de certificación.

Estas obligaciones podrán ser precisadas por la AAC, a excepción de las que señale expresamente la Ley.

Artículo 13°.- Respaldo financiero
Las Entidades de Certificación acreditadas o reconocidas deberán contar con el respaldo económico suficiente para operar bajo la IOFE, así como para afrontar el riesgo de responsabilidad por daños. La AAC determinará los requisitos y cuantía de las pólizas de seguros o garantías bancarias a exigir y los criterios para evaluar el cumplimiento de este requisito.

Artículo 14°.- Del cese de operaciones
La Entidad de Certificación cesa sus operaciones en el marco de la IOFE, en los siguientes casos:

a) Por decisión unilateral comunicada a la AAC, asumiendo la responsabilidad del caso por dicha decisión.
b) Por extinción de su personería jurídica.
c) Por revocación de su registro.
d) Por sentencia judicial.
e) Por liquidación, decidida por la junta de acreedores en el marco de la legislación concursal, o resolución judicial de quiebra.

Para los supuestos contemplados en los incisos a) y b) la AAC establecerá el plazo en el cual las Entidades de Certificación notificarán tanto a aquélla como a los titulares de certificados digitales el cese de sus actividades. La AAC deberá adoptar las medidas necesarias para preservar las obligaciones contenidas en los incisos d), g) e i) del artículo 12° del Reglamento.
La AAC reglamentará los procedimientos para hacer público el cese de operaciones de las entidades de certificación.
Los certificados digitales emitidos por una Entidad de Certificación cuyas operaciones han cesado deben ser cancelados a partir del día, hora, minuto y segundo en que se aplica el cese. El uso de certificados digitales con posterioridad a su cancelación conlleva la inaplicabilidad de los artículos 5° y 6° del presente Reglamento.

CAPÍTULO III
DE LAS ENTIDADES DE REGISTRO O VERIFICACIÓN

Artículo 15°.- Funciones
Las Entidades de Registro o Verificación tienen las siguientes funciones:

a) Identificar al solicitante del certificado digital mediante el levantamiento de datos y la comprobación de la información brindada por aquel.
b) Identificar al solicitante de cualquier otra firma electrónica.
c) Aceptar y/o autorizar, según sea el caso, la conformidad de las solicitudes de emisión, modificación o cancelación de certificados digitales, comunicándolo a la Entidad de Certificación.

Artículo 16°.- Obligaciones
Las Entidades de Registro o Verificación registradas tienen las siguientes obligaciones:

a) Cumplir con su Declaración de Prácticas de Registro o Verificación.
b) Determinar objetivamente y en forma directa la veracidad de la información proporcionada por el solicitante del certificado digital, bajo responsabilidad.
c) Mantener la confidencialidad de la información relativa a los solicitantes y titulares de certificados digitales, limitando su empleo a las necesidades propias del servicio de registro o verificación, salvo orden judicial o pedido expreso del titular del certificado digital.
d) Recoger únicamente información o datos personales de relevancia para la emisión de los certificados.
e) Acreditar domicilio en el Perú.
f) Mantener vigente la contratación de seguros o garantías bancarias que permitan indemnizar al titular por los daños que puedan ocasionar como resultado de las actividades de certificación.

Estas obligaciones podrán ser precisadas por la AAC, a excepción de las que señale expresamente la Ley.

Artículo 17°.- Respaldo financiero
Las Entidades de Registro o Verificación acreditadas deberán contar con el respaldo económico suficiente para operar bajo la IOFE, así como para afrontar el riesgo de responsabilidad por daños, de conformidad con lo dispuesto en la Ley y en el Reglamento. La AAC determinará los requisitos y cuantía de las pólizas de seguros o garantías bancarias a exigir y los criterios para evaluar el cumplimiento de este requisito.

Artículo 18°.- Cese de operaciones
La Entidad de Registro o Verificación cesa de operar en el marco de la IOFE en los siguientes casos:

a) Por decisión unilateral comunicada a la AAC, asumiendo la responsabilidad del caso por dicha decisión.
b) Por extinción de su personería jurídica.
c) Por revocación de su registro.
d) Por sentencia judicial.
e) Por liquidación, decidida por la junta de acreedores en el marco de la legislación concursal o resolución judicial de quiebra.

Para los supuestos contenidos en los incisos a) y b) la Entidad de Registro o Verificación debe notificar el cese de sus actividades a la AAC con una anticipación mínima que será establecida por ésta, debiendo dejar constancia ante aquella de los mecanismos utilizados para preservar el cumplimiento de lo dispuesto en el inciso c) del artículo 16° del Reglamento.

CAPÍTULO IV
DE LA FIRMA DIGITAL

Artículo 19°.- Firma digital
Aquella firma electrónica que utilizando una técnica de criptografía asimétrica, permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su control, de manera que está vinculada únicamente al mismo y a los datos a los que refiere, lo que permite garantizar la integridad del contenido y detectar cualquier modificación ulterior. Tiene la misma validez y eficacia jurídica que el uso de una firma manuscrita.
Las firmas digitales son las generadas a partir de certificados digitales que son:

a) Emitidos conforme a lo dispuesto en el Reglamento por entidades de certificación acreditadas ante la AAC.
b) Incorporados a la IOFE bajo acuerdos de certificación cruzada, conforme al artículo 55° del Reglamento.
c) Reconocidos al amparo de acuerdos de reconocimiento mutuo suscritos por la AAC conforme al artículo 53° del Reglamento.
d) Emitidos por entidades de certificación extranjeras que hayan sido incorporados por reconocimiento a la IOFE conforme al artículo 54° del Reglamento.

Artículo 20°.- Características
Las características mínimas de la firma digital generada bajo la IOFE son:

a) Se genera al cifrar el código de verificación de un mensaje de datos, usando la clave privada del titular del certificado.
b) Es exclusiva del titular de la firma digital y de cada mensaje de datos firmado por éste.
c) Es susceptible de ser verificada usando la clave pública del titular de la firma digital.
d) Su generación está bajo el control exclusivo del titular de la firma digital.
e) Está añadida o asociada lógicamente al mensaje de datos de tal manera que es posible detectar si la firma digital o el mensaje de datos fue alterado.

Artículo 21°.- Funciones
Dadas las características señaladas en el artículo anterior, técnicamente la firma digital debe garantizar que:

a) El mensaje de datos fue enviado y firmado con la clave privada del titular de la firma digital.

b) El mensaje de datos no ha sido alterado después que el remitente lo envió.

c) Como consecuencia de los dos literales previos, el titular de la firma digital no podrá repudiar o desconocer un mensaje de datos que ha sido firmado digitalmente usando su clave privada dado que ésta se mantiene bajo su control exclusivo.

Artículo 22°.- Del titular de la firma digital

Dentro de la IOFE, la responsabilidad sobre los efectos jurídicos generados por la utilización de una firma digital corresponde al titular del certificado.

Tratándose de personas naturales, éstas son titulares del certificado digital y de las firmas digitales que se generen a partir de aquél, incluyendo las firmas digitales que se generen a través de agentes automatizados.

En el caso de personas jurídicas, son éstas los titulares del certificado digital, y sus representantes son los titulares de la firma digital, con excepción de las firmas digitales que se generen a través de agentes automatizados, situación en la cual las personas jurídicas son titulares del certificado y de las firmas digitales generadas a partir de éstos.

Artículo 23°.- Obligaciones del titular

Las obligaciones del titular de la firma digital son:

a) Entregar información veraz bajo su responsabilidad.

b) Generar la clave privada y firmar digitalmente mediante los procedimientos señalados por la Entidad de Certificación.

c) Mantener el control y la reserva de la clave privada bajo su responsabilidad.

d) Observar las condiciones establecidas por la Entidad de Certificación para la utilización del certificado digital y la generación de firmas digitales.

e) En caso de que la clave privada quede comprometida en su seguridad, el titular debe notificarlo de inmediato a la Entidad de Certificación para que cancele el certificado digital. La Entidad de Certificación será responsable de los daños que pueda ocasionar la demora en dicha cancelación.

Artículo 24°.- Invalidez

Una firma digital generada bajo la IOFE pierde validez si es utilizada:

a) En fines distintos para los que fue extendido el certificado.

b) Cuando el certificado haya sido cancelado o revocado conforme a lo establecido en el Capítulo V del presente Título.

CAPÍTULO V
DEL CERTIFICADO

Artículo 25°.- Requisitos

Para la obtención de un certificado digital, el solicitante deberá acreditar lo siguiente:

a) Tratándose de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles.

b) Tratándose de personas jurídicas, acreditar la existencia de la misma y su vigencia mediante los instrumentos públicos o norma legal respectiva.

Artículo 26°.- Especificaciones adicionales para ser titular

Para ser titular de un certificado digital adicionalmente se deberá cumplir con entregar la información solicitada por la Entidad de Registro o Verificación, de acuerdo a lo estipulado por la Entidad de Certificación correspondiente, asumiendo responsabilidad por la veracidad y exactitud de la información proporcionada, sin perjuicio de la respectiva comprobación.

En el caso de personas naturales, la solicitud del certificado digital y el registro o verificación de su identidad son estrictamente personales. La persona natural solicitante se constituirá en titular del certificado digital y de las firmas digitales que se generen.

Para el caso de personas jurídicas, la solicitud del certificado digital del cual ésta será titular y el registro o verificación de su identidad deben ser realizados a través de un representante debidamente acreditado. Conjuntamente con la solicitud debe indicarse el representante, persona natural, al cual se le asignará la facultad de generar y usar la clave privada, señalando para tal efecto las atribuciones y los poderes de representación correspondientes. Dicha persona natural será el titular de las firmas digitales. Tratándose de certificados digitales solicitados por personas jurídicas para su utilización a través de agentes automatizados, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderá a la persona jurídica. La atribución de responsabilidad, para tales efectos, corresponde al representante legal, que en nombre de la persona jurídica solicita el certificado digital.

Artículo 27°.- Procedimiento para ser titular

Para el caso de personas naturales, éstas deberán presentar una solicitud a la Entidad de Registro o Verificación, según sea el caso; dicha solicitud deberá estar acompañada de toda la información requerida por la declaración de prácticas de certificación o en los procedimientos declarados. La Entidad de Registro o Verificación deberá comprobar la identidad del solicitante a través de su documento oficial de identidad. La Entidad de Certificación cumplirá lo dispuesto en el presente artículo, en el supuesto previsto en el segundo párrafo del artículo 12° de la Ley.

En el caso de una persona jurídica, la solicitud deberá ser presentada por la persona facultada para tal fin, debiendo acreditar la existencia y vigencia de la persona jurídica mediante los instrumentos públicos o norma legal respectiva, así como las facultades del representante. Asimismo, deberá presentar toda la información requerida por la declaración de prácticas de la entidad correspondiente.

Artículo 28°.- Obligaciones del titular

a) Actualizar permanentemente la información proveída tanto a la Entidad de Certificación como a la Entidad de Registro o Verificación, asumiendo responsabilidad por la veracidad y exactitud de ésta.

b) Solicitar de inmediato la cancelación de su certificado digital en caso de que la reserva sobre la clave privada se haya visto comprometida, bajo responsabilidad.

c) Observar permanentemente las condiciones establecidas por la Entidad de Certificación para la utilización del certificado.

Artículo 29°.- Contenido y vigencia

Los certificados emitidos dentro de la IOFE deberán contener como mínimo lo establecido en el artículo 7° de la Ley.

La Entidad de Certificación podrá incluir, a pedido del solicitante del certificado información adicional siempre y cuando la Entidad de Registro o Verificación compruebe fehacientemente la veracidad de ésta.

El período de vigencia de los certificados digitales comienza y finaliza en las fechas indicadas en él, salvo en los supuestos de cancelación conforme al artículo 9° de la Ley. Los certificados digitales tendrán una validez máxima de tres (3) años.

Artículo 30°.- Causales de cancelación

La cancelación del certificado puede darse:

a) A solicitud del titular del certificado digital o del titular de la firma digital sin previa justificación, siendo necesario para tal efecto la aceptación y autorización de la Entidad de Certificación o la Entidad de Registro o Verificación, según sea el caso, la misma que deberá ser aceptada y autorizada como máximo dentro del plazo establecido por la AAC. Si en el plazo indicado la entidad no se pronuncia, se entenderá que el certificado ha sido cancelado, sin perjuicio del tercero de buena fe.

b) Por revocación efectuada por la Entidad de Certificación, con expresión de causa.

c) Por expiración del plazo de vigencia.

d) Por el cese de operaciones de la Entidad de Certificación que lo emitió.

e) Por resolución administrativa o judicial que lo ordene.

f) Por interdicción civil judicialmente declarada, declaración de ausencia o de muerte presunta, del titular del certificado.

g) Por extinción de la personería jurídica o declaración judicial de quiebra.

h) Otras causales que establezca la AAC.

i) Por muerte, o por inhabilitacion o incapacidad declarada judicialmente de la persona natural titular del certificado.

Artículo 31°.- Cancelación del certificado a solicitud de su titular

La solicitud de cancelación de un certificado digital puede ser realizada por su titular o a través de un representante debidamente acreditado; pudiendo realizarse mediante documento electrónico firmado digitalmente, de acuerdo con los procedimientos definidos en cada caso por las Entidades de Certificación.

El titular del certificado está obligado, bajo responsabilidad, a solicitar la cancelación al tomar conocimiento de la ocurrencia de alguna de las siguientes circunstancias:

a) Por exposición, puesta en peligro o uso indebido de la clave privada.

b) Por deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada.

Artículo 32°.- Cancelación por revocación

La revocación supone la cancelación de oficio de los certificados por parte de la Entidad de Certificación, quien debe contar con procedimientos detallados en su declaración de prácticas de certificación.

La revocación también puede ser solicitada por un tercero que informe fehacientemente de alguno de los supuestos de revocación contenidos en los numerales 1) y 2) del artículo 10° de la Ley.

La revocación debe indicar el momento desde el cual se aplica, precisando la fecha, hora, minuto y segundo del mismo. La revocación no puede ser aplicada retroactivamente y debe ser notificada al titular del certificado digital. La Entidad de Certificación debe inmediatamente incluir la revocación del certificado digital en la relación que corresponda.

CAPÍTULO VI
CERTIFICACION DIGITAL EN EL SECTOR PÚBLICO

Artículo 33°.- Entidades de Certificación y de Registro o Verificación

En el ámbito del Sector Público, las entidades que presten servicios de certificación digital en el marco de la IOFE, son las siguientes:

a) Entidad de Certificación Nacional para el Estado Peruano (ECERNEP), la cual será la encargada de emitir los certificados raíz para las Entidades de Certificación para el Estado Peruano que lo soliciten, además de proponer las políticas y estándares de las ECEP y EREP según lo establecido por el presente reglamento.

b) Entidades de Certificación para el Estado Peruano (ECEP) acreditadas o reconocidas por la AAC, las cuales serán las encargadas de proporcionar, emitir o cancelar los certificados digitales: i) a los administrados, personas naturales y jurídicas, los cuales serán utilizados únicamente en los trámites, procedimientos administrativos y similares; ii) a los funcionarios, empleados y servidores públicos para el ejercicio de sus funciones y la realización de actos de administración interna e interinstitucional, y a las personas expresamente autorizadas por la entidad pública correspondiente. Cualquier otro uso que no forme parte del ejercicio de las funciones, de los procedimientos administrativos o de administración interna del Estado o de los procedimientos y coordinaciones entre entidades públicas carecerá del respaldo legal de la IOFE.

c) Entidades de Registro o Verificación para el Estado Peruano (EREP) acreditadas o reconocidas por la AAC, serán las encargadas de: levantamiento de datos, comprobación de la información de un solicitante, identificación y autenticación del suscriptor, aceptación y autorización de solicitudes de emisión y cancelación de certificados digitales además de su gestión ante las Entidades de Certificación; para los fines previstos en el inciso b) del presente artículo.

Las entidades señaladas en los incisos a), b) y c) podrán brindar servicios de intermediación electrónica, conforme a lo dispuesto en la Ley y el presente reglamento.

La prestación de los servicios de certificación o de registro y verificación por parte de las entidades de la Administración Pública se sustentan en los principios de acceso universal y no discriminación del uso de las tecnologías de la información y de comunicaciones, procurando que los beneficios resultantes contribuyan a la mejora de la calidad de vida de todos los ciudadanos, así como el acceso gratuito de los servicios. En consecuencia, las entidades públicas que presten sus servicios como ECERNEP, ECEP y EREP, con el fin de determinar el valor de los mismos sólo podrán considerar los costos asociados a su prestación.

Artículo 34°.- Designación de las entidades responsables

Se designa al Registro Nacional de Identificación y Estado Civil - RENIEC como ECERNEP, ECEP y EREP. Los servicios a ser prestados en el cumplimiento de los roles señalados estarán a disposición de todas las Entidades Públicas del Estado Peruano y de todas las personas naturales y personas jurídicas que mantengan vínculos con el mismo, no excluyendo ninguna representación del Estado Peruano en el territorio nacional o en el extranjero.

Las entidades a que se refiere el artículo 33° del Reglamento serán acreditadas y reconocidas por la AAC.

Artículo 35°.- El Documento Nacional de Identidad electrónico

El Documento Nacional de Identidad electrónico (DNIe) es el Documento Nacional de Identidad que acredita presencial y electrónicamente la identidad personal de su titular, permitiendo la firma electrónica de documentos. Este documento se constituye en uno de los medios por los cuales el RENIEC, actuando como ECEP, proveerá los certificados digitales a ser emitidos a los ciudadanos, para los usos en los términos que se señalan en el inciso b) del artículo 33°, del reglamento. A diferencia de los certificados digitales que pudiesen ser provistos por otras ECEP, el que se incorpora en el DNIe cuenta con la facultad adicional de poder ser utilizado para el ejercicio del voto electrónico en los procesos electorales, en la medida que esta alternativa estuviese implementada.

Artículo 36°.- Implementación de otras Entidades de Certificación para el Estado Peruano (ECEP) y Entidades de Registro o Verificación para el Estado Peruano (EREP)

Otras entidades públicas del Estado Peruano, que por sus funciones, facultades o planes estratégicos para la mejora de sus servicios hacia sus usuarios, requieren constituirse en ECEP y/o EREP, deberán acreditarse o ser reconocidas por la AAC, debiendo cumplir con las políticas y estándares propuestos por la ECERNEP para el sector público y que sean compatibles con los estándares establecidos por la AAC.

Artículo 37°.- De la Entidad de Certificación Nacional para el Estado Peruano (ECERNEP)

a) El RENIEC será la única ECERNEP y actuará también como ECEP y EREP.

Todas las ECEP y las EREP deben seguir las políticas y estándares propuestos por la ECERNEP y aprobados

por la AAC, así como aquellos lineamientos definidos por la ONGEI para el Sector Público.

b) A fin de brindar una imagen de plataforma confiable, la ECERNEP deberá, en caso corresponda, realizar las acciones necesarias a fin de registrar su certificado dentro de los principales navegadores de Internet.

c) Deberá soportarse en una estructura funcional y jurídica estable, no cambiante en el mediano plazo, sólo variable en la cantidad de Entidades de Certificación y Registro que pueda tener.

d) La ECERNEP y las ECEP emplearan el grado de seguridad adecuado en la selección del algoritmo, en la longitud de la clave, en el medio de almacenamiento de la clave privada y en la implementación de los algoritmos empleados, así como el contenido de los certificados digitales que permitan interoperabilidad entre las distintas plataformas tecnológicas y sistemas informáticos de firmas digitales, los cuales deberán ser establecidos por la ECERNEP y ser compatibles con las disposiciones establecidas por la AAC.

e) Deberá ser auditada periódicamente por la AAC. Los informes de auditoria deben ser tenidos en cuenta para continuar su operación. Asimismo, en el caso de un proceso de acreditación, la auditoria será previa a la terminación del mismo.

f) Para la acreditación de la ECERNEP ante la AAC, no resultará exigible el requisito de respaldo financiero. Tampoco lo será lo señalado en el inciso n) del artículo 12°.

Artículo 38°.- De las Entidades de Certificación para el Estado Peruano (ECEP)

a) Deberán ofrecer un servicio de directorio y permitir que las aplicaciones accedan a los certificados digitales emitidos y a la Lista de Certificados Digitales Revocados (LCR). Este servicio se debe encontrar actualizado con la frecuencia indicada en las Políticas de Certificación de cada tipo de certificado. Junto al Servicio de Directorio se puede disponer del servicio de consulta en línea del estado de un certificado digital.

b) Una ECEP podrá ofrecer distintos servicios y mecanismos para recibir un requerimiento de certificado digital para otorgar el mismo a su titular. La recepción de solicitudes de revocación y la publicación periódica de la Lista de Certificados Digitales Revocados (LCR) son servicios que debe ofrecer en forma obligatoria. Asimismo, deberá garantizar el acceso permanente a dichos servicios, proponiendo una solución para una eventual contingencia.

c) Deberán ofrecer el servicio de emisión y renovación de certificados digitales.

d) Las ECEP podrán ofrecer y emitir distintos tipos de firmas electrónicas y/o certificados digitales pudiendo soportarse en diversas tecnologías.

e) La estructura de los certificados emitidos por las ECEP deberá ser electrónicamente articulable con todas las aplicaciones y plataformas informáticas que requieran su uso.

f) Se ofrecerá un grado de seguridad adecuado en relación a los equipos informáticos y de comunicación empleados, al personal empleado para operar la ECEP, a los responsables de operar las claves de la ECEP y a los procedimientos utilizados para la autenticación de los datos a ser incluidos en los certificados digitales.

g) La integridad del directorio de certificados digitales y la lista de certificados digitales revocados debe estar permanentemente asegurada. Es responsabilidad de la ECEP garantizar la disponibilidad de este servicio y la calidad de los datos suministrados por éste.

h) Cada titular del certificado deberá ser distinguido unívocamente. Para el caso de los funcionarios, empleados o servidores públicos y de las personas expresamente autorizadas por la entidad pública correspondiente, deberá incluirse en los certificados, el organismo donde desempeñan sus funciones o el organismo por el cual ha sido autorizado. Para los administrados, ciudadanos o empresas deberá incluirse el organismo emisor del certificado.

i) Los campos que indiquen el período de validez o vigencia ("no antes de" y "no después de") deberán detallar la fecha y la hora.

j) Para la acreditación de las ECEP ante la AAC, no resultará exigible el requisito de respaldo financiero. Tampoco lo será lo señalado en el inciso n) del artículo 12°.

Artículo 39°.- Disposiciones generales para el Sector Público

a) Los trámites y procedimientos administrativos ante las entidades de la Administración Pública, la constancia documental de la transmisión a distancia por medios electrónicos entre autoridades administrativas o con sus administrados, o cualquier tramite, procedimiento o proceso por parte de los administrados o ciudadanos ante las Entidades Publicas o entre estas entidades, no excluyendo a las representaciones del Estado Peruano en el exterior, podrán efectuarse utilizando las diversas tecnologías de certificados digitales y firmas electrónicas reconocidas por la AAC, conforme a Ley.

b) Las entidades de la administración pública deberán admitir la recepción de documentos digitales firmados digitalmente utilizando certificados digitales emitidos por entidades de certificación acreditadas o reconocidas por la AAC, públicas o privadas, indistintamente.

c) Todas las disposiciones y regulaciones complementarias para la aplicación de las diversas tecnologías de firmas electrónicas y certificados digitales en el sector público para el uso en los sistemas informáticos o aplicativos orientados al desarrollo de la Sociedad de la Información y el Gobierno Electrónico en el Estado Peruano, como el Sistema Electrónico de Contrataciones y Adquisiciones del Estado-SEACE, Voto Electrónico, entre otros, serán definidas y establecidas por Oficina Nacional de Gobierno Electrónico e Informática y aprobadas por la Presidencia del Consejo de Ministros, con el objetivo de garantizar un nivel apropiado de seguridad y confianza acorde con las mejores prácticas y estándares vigentes internacionalmente, así como las orientadas a permitir la interoperabilidad entre las diversas plataformas, sistemas o aplicativos informáticos de las la Administración Pública.

d) Los servicios de intermediación electrónica, pueden ser implementados por una institución pública u organismo independiente, caso contrario serán desarrollados por la misma Entidad.

e) Cuando por primera vez un solicitante requiera ante una EREP que se le emita un certificado digital, deberá acreditarse personalmente para dicho propósito.

f) En concordancia con el artículo 36°, las entidades públicas del Estado Peruano, que por sus funciones, facultades o planes estratégicos para la mejora de sus servicios hacia sus administrados, requieran utilizar funcionalidades de firma digital en sus sistemas o aplicativos informáticos para brindar confianza e interoperabilidad entre otras plataformas del Estado, pudiendo a voluntad constituirse en ECEP, podrán obtener el Certificado Raíz de la ECERNEP, para lo cual deberán seguir las políticas y estándares para el sector público establecidas por la ECERNEP.

g) Todas las disposiciones de la Ley y el Reglamento son aplicables a la ECERNEP, las ECEP y las EREP, en lo que corresponda.

h) Para la acreditación de las EREP ante la AAC, no resultará exigible el requisito de respaldo financiero. Tampoco lo será lo señalado en el inciso f) del artículo 16°.

TÍTULO III

DE LA AUTORIDAD ADMINISTRATIVA COMPETENTE

CAPÍTULO I
DE LAS FUNCIONES

Artículo 40°.- Funciones

La Autoridad Administrativa Competente (AAC) tiene las siguientes funciones:

a) Aprobar la política de certificados y las declaraciones de prácticas de certificación.

b) Acreditar Entidades de Certificación nacionales y reconocer a las Entidades de Certificación extranjeras.

c) Acreditar Entidades de Registro o de Verificación.

d) Registrar a las entidades acreditadas señaladas en los incisos b) y c) del presente artículo, en el Registro de Entidades de Certificación y Entidades de Registro o Verificación previsto en el artículo 15° de la Ley.

e) Supervisar a las Entidades de Certificación, a las Entidades de Registro o Verificación y a los prestadores de servicios de intermediación electrónica.

f) Cancelar las acreditaciones otorgadas a las Entidades de Certificación y a las Entidades de Registro o Verificación conforme a lo dispuesto en el Reglamento.

g) Publicar, por medios telemáticos, la relación de entidades acreditadas.

h) Aprobar el empleo de estándares técnicos internacionales dentro de la Infraestructura Oficial de Firma Electrónica y determinar la compatibilidad de otros estándares técnicos con los estándares internacionales; cooperar, dentro de su competencia, en la unificación de los sistemas que se manejan en los organismos de la Administración Pública, tendiendo puentes entre todos sus niveles; y en la obtención de la interoperabilidad del mayor número de aplicaciones y plataformas de firmas electrónicas.

i) Formular los criterios para el establecimiento de la idoneidad técnica que deberán cumplir quienes presten servicios en las materias reguladas por la Ley y el Reglamento, así como aquellas relacionadas con la prevención y solución de conflictos.

j) Establecer los requisitos mínimos para la prestación de los servicios de certificación y los servicios de registro o verificación.

k) Impulsar la solución de conflictos por medio de la conciliación y el arbitraje.

l) Definir los criterios para evaluar la suficiencia del respaldo financiero con el que deben contar las entidades de certificación y las entidades de registro o verificación.

m) Suscribir acuerdos de reconocimiento mutuo con Autoridades Administrativas Extranjeras que cumplen funciones similares a las de la AAC.

n) Autorizar la realización de certificaciones cruzadas con entidades de certificación extranjeras.

o) Fomentar y coordinar el uso y desarrollo de la Infraestructura Oficial de Firma Electrónica en las entidades del sector público nacional en coordinación con la Entidad de Certificación Nacional para el Estado Peruano (ECERNEP) que se designe.

p) Aprobar y regular los servicios de valor de intermediación digital al interior de la Infraestructura Oficial de Firma Electrónica.

q) Delegar a terceros bajo sus órdenes y responsabilidad, y a la Entidad de Certificación Nacional para el Estado Peruano (ECERNEP) designada, las funciones que estime pertinentes conforme a lo previsto en el presente reglamento.

r) Sancionar a las Entidades de Certificación, a las Entidades de Registro o Verificación o a los prestadores de servicios de intermediación electrónica, por el incumplimiento o infracción al presente reglamento y demás disposiciones vinculadas a la Infraestructura Oficial de Firma Electrónica.

s) Las demás que sean necesarias para el buen funcionamiento de la infraestructura Oficial de Firma Electrónica.

CAPÍTULO II

DEL RÉGIMEN DE ACREDITACIÓN DE ENTIDADES DE CERTIFICACION Y DE LAS ENTIDADES DE REGISTRO O VERIFICACIÓN

Artículo 41°.- Acreditación de Entidades de Certificación

Las entidades que soliciten su acreditación y registro ante la AAC, como Entidades de Certificación, incluyendo las ECEP, deben contar con los elementos de la IOFE señalados en los incisos b), c) y d) del artículo 9° y someterse al procedimiento de evaluación comprendido en el artículo 45° del reglamento.

Cuando alguno de los elementos señalados en el párrafo precedente sea administrado por un tercero, la entidad solicitante deberá demostrar su vinculación con aquél, asegurando la viabilidad de sus servicios bajo dichas condiciones, y la disponibilidad de estos elementos para la evaluación y supervisión que la AAC considere necesarias. La AAC, de ser el caso, precisará los términos bajo los cuales se rigen estos supuestos del servicio de certificación.

Los Notarios Públicos pueden solicitar su acreditación como Entidad de Registro o Verificación en la prestación de los servicios de certificación digital, debiendo cumplir con los requisitos estipulados en el presente reglamento y la Ley.

Artículo 42°.- Presentación de la solicitud de acreditación de la entidad de certificación

La solicitud de acreditación de Entidades de Certificación debe presentarse a la AAC, observando lo dispuesto en el artículo anterior y adjuntando lo siguiente:

a) Pago por derecho de solicitud de acreditación por un monto equivalente al 100% de la UIT vigente a la fecha de pago.

b)Acreditación de la existencia y vigencia de la persona jurídica mediante los instrumentos públicos o norma legal respectiva, así como las facultades del representante.

c) Acreditar domicilio en el país.

d) Acreditar contar con la. infraestructura e instalaciones necesarias para la prestación del servicio y presentar declaración jurada de aceptación de la visita comprobatoria de la AAC.

e) Declaración de prácticas de certificación y documentación que comprende el sistema de gestión implementado conforme al inciso b) del artículo 9° del Reglamento.

f) Declaración jurada del cumplimiento de los requisitos señalados en los Incisos c) y d) del artículo 9° del Reglamento; información qué será comprobada por parte de la AAC.

g) Documentación que acredite el cumplimiento de lo dispuesto en los artículos 12° y 13° del Reglamento y demás que la AAC señale.

h) Informe favorable de la entidad sectorial correspondiente, cuando lo solicite la AAC, para el caso de personas jurídicas supervisadas, respecto de la legalidad y seguridad para el desempeño de actividades de certificación.

Artículo 43°.- Acreditación de Entidades de Registro o Verificación

Las entidades que soliciten su acreditación y registro ante la AAC, como Entidades de Registro o Verificación, incluyendo las EREP, deben contar con procedimientos para la prestación de sus servicios, los mismos que tendrán que asegurar la verificación presencial de la identidad del solicitante de un nuevo certificado digital.

Artículo 44°.- Presentación de la solicitud de acreditación de Entidades de Registro o Verificación

La solicitud para la acreditación de Entidades de Registro o Verificación debe presentarse a la AAC, observando lo dispuesto en el artículo anterior y adjuntando la información y documentos siguientes:

a) Pago por derecho de solicitud de acreditación por un monto equivalente al 100% de la UIT, vigente.

b) Acreditación de la existencia y vigencia de la persona jurídica mediante los instrumentos públicos o norma legal respectiva, así como las facultades del representante. Acreditar domicilio en el país.

c) Acreditar contar con la infraestructura e instalaciones necesarias para la prestación del servicio y presentar declaración jurada de aceptación de las visitas comprobatorias de la AAC.

d) Procedimientos detallados que garanticen el cumplimiento de las funciones establecidas en el Reglamento.

e) Declaración de prácticas de registro o verificación.

f) Declaración jurada del cumplimiento de los requisitos señalados en los artículos 16° y 17° del Reglamento.

Artículo 45°.- Procedimiento Administrativo de la Acreditación

Admitida la solicitud, la AAC procederá a la evaluación del cumplimiento de los requisitos establecidos en la Ley como en el Reglamento.

La evaluación de los requisitos de competencia técnica de la Entidad de Certificación o de Registro o Verificación solicitante podrá ser realizada directamente por la AAC, o a través de terceros, o reconociendo aquellas realizadas en el extranjero por otras Autoridades Extranjeras que cumplan funciones equivalentes a las de la AAC, y siempre que los requisitos evaluados por ellas sean equivalentes a los requisitos comprendidos en el Reglamento, para lo cual la AAC adoptará los requerimientos, estándares y procedimientos empleados a nivel internacional para la realización de esta función.

Artículo 46°.- Reconocimiento de evaluaciones en el extranjero

La AAC reconocerá las evaluaciones sobre los requisitos de competencia técnica de la Entidad de Certificación solicitante realizadas en el extranjero siempre y cuando se cumplan con las normas establecidas por la AAC en el marco del Reglamento.

Artículo 47°.- Subsanación de observaciones

Dentro del procedimiento podrán subsanarse las deficiencias técnicas observadas durante la evaluación. Las entidades podrán solicitar la suspensión del procedimiento a fin de implementar las medidas necesarias para superar estas dificultades.

Si, culminada la etapa de evaluación, se mantienen observaciones, se denegará el Registro y se archivará el procedimiento.

Artículo 48°.- Costos del Registro y otros procedimientos

Las entidades solicitantes asumirán los costos por la tramitación del procedimiento, y aquellos por evaluación, auditoría y demás previstos por la AAC.

Artículo 49°.- Otorgamiento y vigencia de la acreditación

La acreditación se otorga por un período de tres (3) años, renovable por períodos similares. La Entidad beneficiaria estará sujeta a evaluaciones técnicas anuales para mantener la vigencia de la referida acreditación.

Artículo 50°.- Cancelación de la Acreditación

La cancelación de la acreditación de las Entidades de Certificación o de las Entidades de Registro o Verificación procede:

a) Por decisión unilateral comunicada a la AAC.
b) Por extinción de su personería jurídica.
c) Por revocación de su registro.
d) Por sentencia judicial.
e) Por liquidación, decidida por la junta de acreedores en el marco de la legislación concursal o resolución judicial de quiebra.

CAPÍTULO III

DE LA INTERMEDIACIÓN ELECTRÓNICA

Artículo 51°.- De los servicios de intermediación electrónica

Los servicios de intermediación electrónica a los que acceden voluntariamente y por acuerdo entre las partes en la transmisión de un mensaje de datos o documento electrónicos que utilizan firmas electrónicas, son brindados por prestadores autorizados que deberán estar inscritos y registrados en la AAC.

El prestador de servicios de intermediación electrónica estará habilitado para ejercer sus funciones por un plazo renovable de tres (3) años a partir de su inscripción en la AAC.

Artículo 52°.- De la inscripción para la prestación de servicios de intermediación electrónica:

Los requisitos para la prestación de servicios de intermediación electrónica son:

a) Pago por derecho de solicitud de acreditación por un monto equivalente al 100% de la UIT.
b) Acreditación de la vigencia en el caso de persona jurídica.
c) Acreditar domicilio en el país.
d) Acreditar contar con la infraestructura y capacidad tecnológica para la prestación de los servicios de intermediación electrónica de conformidad con las exigencias previstas en las normas técnicas peruanas vigentes.
e) Declaración jurada de aceptación de auditorías cuando la AAC lo requiera.
f) Cumplir los demás requisitos exigidos por la AAC.

CAPÍTULO IV

DE LOS CERTIFICADOS EMITIDOS POR ENTIDADES EXTRANJERAS

Artículo 53°.- Acuerdos de reconocimiento mutuo

La AAC podrá suscribir acuerdos de reconocimiento mutuo con entidades similares, a fin de reconocer la validez de los certificados digitales otorgados en el extranjero y extender la interoperabilidad de la IOFE. Los acuerdos de reconocimiento mutuo deben garantizar en forma equivalente las funciones exigidas por la Ley y su Reglamento.

Artículo 54°.- Reconocimiento

La AAC podrá reconocer los certificados digitales emitidos por Entidades Extranjeras, de acuerdo con las prácticas y políticas que para tal efecto apruebe, las que deben velar por el cumplimiento de las obligaciones y responsabilidades establecidas en el Reglamento u otra norma posterior. Asimismo, podrá autorizar la operación de aquellas Entidades de Certificación nacionales que utilicen los servicios de Entidades de Certificación extranjera, de verificarse tal supuesto, las entidades nacionales asumirán las responsabilidades del caso.

Para tal efecto, la entidad extranjera deberá comunicar a la AAC el nombre de aquellas entidades de certificación que autorizarán las solicitudes de emisión de certificados digitales así como la gestión de los mismos.

La AAC emitirá las normas que aseguren el cumplimiento de lo establecido en el presente artículo; así como los mecanismos adecuados de información a los agentes del mercado.

Artículo 55°.- Certificación cruzada

Las Entidades de Certificación acreditadas pueden realizar certificaciones cruzadas con Entidades de Certificación Extranjeras a fin de reconocer los certificados digitales que éstas emitan en el extranjero, incorporándolos como suyos dentro de la IOFE, siempre y cuando obtengan autorización previa de la AAC.

Las entidades que presten servicios de acuerdo a lo establecido en el párrafo precedente, asumirán responsabilidad de daños y perjuicios por la gestión de tales certificados.

Las Entidades de Certificación acreditadas que realicen certificaciones cruzadas conforme al primer párrafo del presente artículo, garantizarán ante la AAC que las firmas electrónicas y/o certificados digitales reconocidos han sido emitidos bajo requisitos equivalentes a los exigidos en la IOFE, y que cumplen las funciones señaladas en el artículo 2° de la Ley.

CAPÍTULO V

DE LA SUPERVISIÓN DE ENTIDADES ACREDITADAS

Artículo 56°.- Facultades de Supervisión

La AAC tiene la facultad de verificar la correcta prestación de los servicios de certificación y/o emisión de

firmas electrónicas así como de los servicios de registro o verificación y el cumplimiento de las obligaciones legales y técnicas por parte de las entidades acreditadas que operen bajo la IOFE, así como la facultad de verificar el cumplimiento de las disposiciones establecidas en la Ley, el Reglamento, y en sus Resoluciones.

Artículo 57°.- Aporte por Supervisión y Control Anual

De conformidad con la Ley N° 28403, la AAC recaudará de las entidades privadas de certificación y de verificación o registro acreditadas bajo su ámbito, un aporte por supervisión y control anual, el cual no podrá exceder del 0.8% del valor de la facturación anual, deducido del Impuesto General a las Ventas y el Impuesto de Promoción Municipal.

Artículo 58°.- Fiscalización

La AAC ejercerá su facultad fiscalizadora y sancionadora de conformidad con lo dispuesto en el Decreto Ley N° 25868. Las sanciones a aplicar son determinadas por la AAC en el marco de la Decisión Andina 562 dada la naturaleza de reglamento técnico de la presente norma.

DISPOSICIONES FINALES

Primera.- Cooperación Internacional

Las entidades del Sector Público Nacional pueden suscribir acuerdos de cooperación con sus similares a nivel mundial o con instituciones de cooperación internacional, para recibir apoyo, asesoría y financiamiento para el desarrollo de las firmas electrónicas y transacciones electrónicas en general en la Administración Publica. Encargándose al Consejo Nacional de Ciencia Tecnología e Innovación Tecnológica - CONCYTEC para que en coordinación con la ECERNEP, la Oficina Nacional de Gobierno Electrónico e Informática - ONGEI y la AAC desarrolle las acciones tendientes, dentro del marco de la investigación e innovación tecnológica, a masificar el uso de las firmas electrónicas en las Administración Publica.

Segunda.- Procedimiento administrativo contra decisiones de las Entidades de Certificación

Las Entidades de Certificación deben establecer procedimientos ágiles y sencillos para que sus usuarios puedan presentar directamente reclamaciones por la prestación de sus servicios, las mismas que deberán ser atendidas en el más breve plazo. La AAC aprueba o reforma estos procedimientos y regula todo lo relativo a las reclamaciones. Agotada la vía previa de la reclamación ante la entidad de certificación, procede recurrir en vía administrativa ante la AAC, con sujeción a la Ley N° 27444 - Ley del Procedimiento Administrativo General. La AAC determinará todos aquellos procedimientos y políticas necesarios para la aplicación del Reglamento. En los casos que proceda la reclamación, adoptará las medidas correctivas pertinentes.

Tercera.- Avances Tecnológicos

Dentro del marco conformado por la Ley y el presente Reglamento, la AAC podrá apoyarse en la Comisión de Reglamentos Técnicos y Comerciales del INDECOPI y en las resoluciones que ésta emita y que sean necesarias para mantener la normativa compatible con la evolución tecnológica de la materia y el desarrollo de las necesidades de los usuarios de la Infraestructura Oficial de Firma Electrónica. Asimismo la AAC, procederá a modificar o sustituir las "Disposiciones Complementarias al Reglamento de la Ley de Firmas y Certificados Digitales" aprobadas por la Resolución Comisión de Reglamentos Técnicos y Comerciales N° 0103-2003/CRT-INDECOPI del 23 de octubre de 2003, para compatibilizarlas dentro del marco de este reglamento.

Cuarta.- Almacenamiento digital

Los notarios y fedatarios públicos o particulares, autorizados de conformidad con el Decreto Legislativo N° 681 y sus normas modificatorias y reglamentarias podrán brindar el servicio almacenamiento digital de documentos.

En el caso de las entidades públicas, las oficinas de informática y sistemas o quien haga sus veces serán responsables del archivo digital de la documentación institucional y de su autenticidad, así como de aquella en la cual interviene el fedatario institucional de conformidad con lo previsto en el artículo 127° de la Ley N° 27444, Ley del Procedimiento Administrativo General. Para estos efectos el titular de las mencionadas oficinas utilizará la firma digital en los términos del artículo 19 del presente Reglamento.

Mediante Decreto Supremo refrendado por el Presidente del Consejo de Ministros se podrán establecer criterios para regular el archivo digital de documentos en el ámbito de la Administración Pública.

Quinta.- Disposiciones complementarias de la Ley N° 28403.

Las normas y disposiciones complementarias de la Ley N° 28403 deberán ser dadas por Decreto Supremo refrendado por el Presidente del Consejo de Ministros.

Sexta.- Adecuación del Texto Único de Procedimientos Administrativos del Instituto Nacional de Defensa de la Competencia y de la Propiedad Intelectual (INDECOPI)

En un plazo no mayor de 45 días calendario contados a partir de la vigencia del presente Reglamento, se deberá adecuar de acuerdo a Ley, el Texto Único de Procedimientos Administrativos del Instituto Nacional de Defensa de la Competencia y de la Propiedad Intelectual (INDECOPI), incorporando los procedimientos correspondientes en su calidad de Autoridad Administrativa Competente de la IOFE.

Sétima.- Plazo de Implementación

El RENIEC tendrá un plazo no mayor de 1 (un) año a partir de la vigencia del presente Reglamento, para implementar y poner al servicio de las personas naturales, de las personas jurídicas y de las entidades del Estado, la infraestructura indicada en el artículo 34° del presente Reglamento.

Después de vencido el plazo, la ECERNEP emitirá los certificados raíz correspondientes a las ECEP acreditadas o reconocidas por la AAC, con el fin de garantizar la interoperabilidad y la confianza en el uso de los certificados digitales emitidos por las mismas.

Octava.- Glosario de Términos

De conformidad con lo establecido por la segunda disposición complementaria, transitoria y final de la Ley, se incluye el Glosario de Términos siguiente:

Acreditación.- Acto a través del cual la Autoridad Administrativa Competente, previo cumplimiento de las exigencias establecidas en la Ley, en el Reglamento y en las disposiciones dictadas por ella, faculta a las entidades solicitantes reguladas en el Reglamento a prestar los servicios solicitados en el marco de la Infraestructura Oficial de Firma Electrónica.

Agente Automatizado.- Procesos y equipos programados para atender requerimientos predefinidos y dar una respuesta automática sin intervención humana, en dicha fase.

Autenticación.- Proceso técnico que permite determinar la identidad de la persona que firma electrónicamente, en función del mensaje firmado por éste y al cual se le vincula; este proceso no otorga certificación notarial ni fe pública.

Autoridad Administrativa Competente (AAC).- Organismo público responsable de acreditar a las entidades de certificación y a las entidades de registro o verificación, de reconocer los estándares tecnológicos aplicables en la Infraestructura Oficial de Firma Electrónica, de supervisar dicha Infraestructura, y las otras funciones señaladas en el Reglamento o aquellas que requiera en el transcurso

de sus operaciones. Dicha responsabilidad recae en el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - INDECOPI.

Certificación Cruzada.- Acto por el cual una certificadora acreditada reconoce la validez de un certificado emitido por otra, sea nacional, extranjera o internacional, previa autorización de la Autoridad Administrativa Competente; y asume tal certificado como si fuera de propia emisión, bajo su responsabilidad.

Certificado Digital.- Documento electrónico generado y firmado digitalmente por una entidad de certificación el cual vincula un par de claves con una persona natural o jurídica confirmando su identidad.

Clave Privada.- Es un sistema de criptografía asimétrica que se emplea para generar una firma electrónica sobre un mensaje de datos y es mantenida en reserva por el titular de la firma electrónica.

Clave Pública.- En un sistema de criptografía asimétrica, que es usada por el destinatario de un mensaje de datos para verificar la firma electrónica puesta en dicho mensaje. La clave pública puede ser conocida por cualquier persona.

Código de verificación.- Secuencia de bits de longitud fija obtenida como resultado de procesar un mensaje de datos con un algoritmo, de tal manera que: (1) El mensaje de datos produzca siempre el mismo código de verificación cada vez que se le aplique dicho algoritmo. (2) Sea improbable, a través de medios técnicos, que el mensaje de datos pueda ser derivado o reconstruido a partir del código de verificación producido por el algoritmo. (3) Sea improbable que, por medios técnicos, se pueda encontrar dos mensajes de datos que produzcan el mismo código de verificación al usar el mismo algoritmo.

Criptografía Asimétrica.- Rama de las matemáticas aplicadas que se ocupa de transformar mensajes en formas aparentemente ininteligibles y devolverlas a su forma original, las cuales se basan en el empleo de funciones algorítmicas para generar dos "claves" diferentes pero matemáticamente relacionadas entre sí. Una de esas claves se utiliza para crear una firma numérica o transformar datos en una forma aparentemente ininteligible (clave privada), y la otra para verificar una firma numérica o devolver el mensaje a su forma original (clave pública). Las claves están matemáticamente relacionadas de tal modo que cualquier de ellas implica la existencia de la otra, pero la posibilidad de acceder a la clave privada a partir de la pública es técnicamente ínfima.

Declaración de Prácticas de Certificación.- Documento oficialmente presentado por una entidad de certificación a la Autoridad Administrativa Competente, mediante el cual define sus Prácticas de Certificación.

Declaración de Prácticas de Registro o Verificación.- Documento oficialmente presentado por una Entidad de Registro o Verificación a la Autoridad Administrativa Competente, mediante el cual define sus Prácticas de Registro o Verificación.

Depósito de Certificados.- Sistema de almacenamiento y recuperación de certificados, así como de la información relativa a éstos, disponible por medios telemáticos.

Destinatario.- Persona designada por el iniciador para recibir un mensaje de datos o un documento electrónico, siempre y cuando no actúe a título de intermediario.

Documento.- Cualquier escrito público o privado, los impresos, fotocopias, facsímil o fax, planos, cuadros, dibujos, fotografías, radiografías, cintas cinematográficas, microformas tanto en la modalidad de microfilm como en la modalidad de soportes informáticos, y otras reproducciones de audio o video, la telemática en general y demás objetos que recojan, contengan o representen algún hecho, o una actividad humana o su resultado.

Los documentos pueden ser archivados a través de medios electrónicos, ópticos o cualquier otro similar.

Entidad de Certificación.- Persona jurídica pública o privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de registro o verificación.

Entidad de Certificación Extranjera.- La que no se encuentra domiciliada en el país, ni inscrita en los Registros Públicos del Perú, conforme a la legislación de la materia.

Entidad de Registro o Verificación.-Persona jurídica, con excepción de los notarios públicos, encargada del levantamiento de datos, la comprobación de éstos respecto a un solicitante de un mecanismo de firma electrónica o certificado digital, la aceptación y autorización de las solicitudes para la emisión de un mecanismo de firma electrónica o certificados digitales, así como de la aceptación y autorización de las solicitudes de cancelación de mecanismos de firma electrónica o certificados digitales. Las personas encargadas de ejercer la citada función serán supervisadas y reguladas por la normatividad vigente.

Estándares Técnicos Internacionales.- Requisitos de orden técnico y de uso internacional que deben observarse en la emisión de firmas electrónicas y en las prácticas de certificación.

Estándares Técnicos Nacionales.- Estándares técnicos aprobados mediante Normas Técnicas Peruanas por la Comisión de Reglamentos Técnicos y Comerciales - CRT del INDECOPI, en su calidad de Organismo Nacional de Normalización.

Infraestructura Oficial de Firma Electrónica (IOFE).- Sistema confiable, acreditado, regulado y supervisado por la Autoridad Administrativa Competente, provisto de instrumentos legales y técnicos que permiten generar firmas electrónicas y proporcionar diversos niveles de seguridad respecto a: 1) la integridad de los mensajes de datos y documentos electrónicos; 2) la identidad de su autor, lo que es regulado conforme a Ley. El sistema incluye la generación de firmas electrónicas, en la que participan entidades de certificación y entidades de registro o verificación acreditadas ante la Autoridad Administrativa Competente incluyendo a la Entidad de Certificación Nacional para el Estado Peruano (ECERNEP), las Entidades de Certificación para el Estado Peruano (ECEP) y las Entidades de Registro o Verificación para el Estado Peruano (EREP).

Integridad.- Característica que indica que un mensaje de datos o un documento electrónico no han sido alterados desde la transmisión por el iniciador hasta su recepción por el destinatario.

Lista de Certificados Digitales Revocados (LCR).- Es aquella en la que se deberán incorporar todos los certificados cancelados o revocados por la entidad de certificación de acuerdo con lo establecido en el presente Reglamento.

Mecanismos de Firma Electrónica.- Un programa informático configurado o un aparato informático configurado que sirve para aplicar los datos de creación de firma. Dichos mecanismos varían según el nivel de seguridad que se les aplique.

Medios Telemáticos.- Conjunto de bienes y elementos técnicos informáticos que en unión con las telecomunicaciones permiten la generación, procesamiento, transmisión, comunicación y archivo de datos e información.

Mensaje de Datos.- Es la información generada, enviada, recibida, archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI por sus siglas en inglés), el correo electrónico, el telegrama, el télex o el telefax, entre otros.

Neutralidad Tecnológica.- Principio de no discriminación entre la información consignada sobre papel y la información comunicada o archivada electrónicamente, asimismo la no discriminación, preferencia o restricción de ninguna de las diversas técnicas o tecnologías que pueden utilizarse para firmar, generar, comunicar, almacenar o archivar electrónicamente información.

Niveles de Seguridad.- Son los diversos niveles de garantía que ofrecen las variedades de firmas electrónicas, cuyos beneficios y riesgos deben ser evaluados por la persona, empresa o institución que piensa optar por una modalidad de firma electrónica para enviar o recibir mensajes de datos o documentos electrónicos.

Par de Claves.- En un sistema de criptografía asimétrica, comprende una clave privada y su correspondiente clave pública, ambas asociadas matemáticamente.

Reconocimiento de Servicios de Certificación Prestados en el Extranjero.- Proceso a través del cual la Autoridad Administrativa Competente, acredita, equipara y reconoce oficialmente a las entidades de certificación extranjeras.

Reglamento.- El presente Reglamento de la Ley Nº 27269 - Ley de Firmas y Certificados Digitales, modificada por la Ley Nº 27310.

Servicio de Intermediación Electrónica.- Servicios de valor añadido complementarios de la firma digital brindado dentro o fuera de la Infraestructura Oficial de Firma Electrónica que permiten grabar, almacenar, conservar cualquier información remitida por medios electrónicos que permiten certificar los datos de envío y recepción, su fecha y hora, el no repudio en origen y de recepción. El servicio de intermediación electrónica dentro de la Infraestructura Oficial de Firma Digital es brindado por persona natural o jurídica acreditada ante la Autoridad Administrativa Competente.

Titular de Certificado Digital.- Persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital.

Titular de Firma Electrónica.- Persona natural a quien se le vincula de manera exclusiva con un mensaje de datos firmado electrónicamente utilizando su clave privada. Por excepción, en el caso de firmas digitales generadas a través de agentes automatizados, se considera titular de la firma digital a la persona natural o jurídica titular del certificado a partir del cual se generan dichas firmas digitales.

15539-14

Encargan el Despacho de la Presidencia de la República a la Segunda Vicepresidenta

RESOLUCIÓN SUPREMA
Nº 008-2007-PCM

Lima, 12 de enero de 2007

CONSIDERANDO:

Que, el señor Presidente Constitucional de la República, doctor Alan García Pérez, viajará a la República del Ecuador, el día 15 de enero del presente año, con la finalidad de participar en las Ceremonias de Transmisión de Mando Presidencial en dicho país;

Que el señor Luis Giampietri Rojas, Primer Vicepresidente de la República, ha solicitado no asumir las funciones del Despacho de la Presidencia de la República, por tener que atender asuntos de índole personal el día 15 de enero de 2007;

Que, en consecuencia, es necesario encargar las funciones del Despacho de la Presidencia de la República a la señora Zoila Lourdes Mendoza del Solar, Segunda Vicepresidenta de la República, en tanto dure la ausencia del señor Presidente de la República;

De conformidad con el Artículo 115º de la Constitución Política del Perú; y,

Estando a lo acordado;

SE RESUELVE:

Artículo 1º.- Encargar el Despacho de la Presidencia de la República a la señora Zoila Lourdes Mendoza del Solar, Segunda Vicepresidenta de la República, a partir del día 15 de enero de 2007 y en tanto dure la ausencia del señor Presidente de la República.

Artículo 2º.- La presente Resolución Suprema será refrendada por el Presidente del Consejo de Ministros.

Regístrese, comuníquese y publíquese.

ALAN GARCÍA PÉREZ
Presidente Constitucional de la República

JORGE DEL CASTILLO GÁLVEZ
Presidente del Consejo de Ministros

15581-1

Ratifican contenido de resoluciones por las que se crearon Comisiones Técnicas encargadas del análisis y revisión de normatividad vigente en materia de incautación y decomiso de bienes muebles a favor del Estado y de la Ley Nº 24973

RESOLUCIÓN MINISTERIAL
Nº 418-2006-PCM

Lima, 22 de noviembre de 2006

Visto el Oficio Nº 2398-2006-JUS/SG de la Secretaría General del Ministerio de Justicia;

CONSIDERANDO:

Que, mediante Resolución Ministerial Nº 245-2006-JUS se conformó la Comisión Técnica encargada del análisis y revisión de la normatividad legal y reglamentaria vigente en materia de incautación y decomiso de bienes muebles e inmuebles a favor del Estado, con la finalidad de proponer normas para su sistematización, unificación y ordenación;

Que, de igual modo, mediante Resolución Ministerial Nº 254-2006-JUS se conformó la Comisión Técnica encargada del análisis y revisión de la Ley Nº 24973, que creó el Fondo Indemnizatorio de Errores Judiciales y Detenciones Arbitrarias;

Que, el artículo 5º del Decreto Ley Nº 21292 dispone que las comisiones de carácter multisectorial son conformadas por Resolución del Presidente del Consejo de Ministros;

Que, en salvaguarda de la importante labor que han venido cumpliendo las referidas comisiones técnicas; y a efecto de cumplir con la formalidad establecida por la norma antes citada, es necesario que se ratifique la conformación de las mismas, así como las demás disposiciones que se le vinculan;

De conformidad con lo establecido en el Decreto Legislativo Nº 560 – Ley del Poder Ejecutivo y el Decreto Ley Nº 21292;